Informační a organizační bezpečnost ve zdravotnickém zařízení

Martina Hajdová

Bakalářská práce
2016

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav krizového řízení
akademický rok: 2015/2016

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Martina Hajdová**
Osobní číslo:	**L13182**
Studijní program:	**B3909 Procesní inženýrství**
Studijní obor:	**Ovládání rizik**
Forma studia:	**kombinovaná**

Téma práce: **Informační a organizační bezpečnost ve zdravotnickém zařízení**

Zásady pro vypracování:

1. **Zpracujte průzkum literárních pramenů a zpracujte teoretické poznatky týkající se informační a organizační bezpečnosti.**
2. **Analyzujte a zhodnoťte informační a organizační bezpečnost ve vybraném zdravotnickém zařízení.**
3. **Navrhněte a formulujte doporučení pro zlepšení informační a organizační bezpečnosti ve vybraném zdravotnickém zařízení.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

[1] DOUCEK, Petr. Řízení bezpečnosti informací: 2. rozšířené vydání o BCM. 2., přeprac. vyd. Praha: Professional Publishing, 2011, 286 s. ISBN 9788074310508.

[2] MATOUŠOVÁ, Miroslava a Ladislav HEJLÍK. Osobní údaje a jejich ochrana. 2., dopl. a aktualiz. vyd. Praha: ASPI, 2008, 455 s. ISBN 978-80-7357-322-5.

[3] NOVÁK, Daniel. Zákon o ochraně osobních údajů a předpisy související: komentář. Vyd. 1. Praha: Wolters Kluwer, 2014, xx, 484 s. Komentáře (Wolters Kluwer ČR). ISBN 9788074786655.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **prof. Ing. Jiří Dvořák, DrSc.**
Ústav krizového řízení

Datum zadání bakalářské práce: **5. února 2016**

Termín odevzdání bakalářské práce: **9. května 2016**

V Uherském Hradišti dne 12. února 2016

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta logistiky a krizového řízení
L.S.

doc. RNDr. Jiří Dostál, CSc.
děkan

Ing. et Ing. Jiří Konečný, Ph.D.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

V Uherském Hradišti

.....
podpis studenta

ABSTRAKT

Bakalářská práce se zabývá problematikou ochrany citlivých dat pacientů ve zdravotnictví. Teoretická část charakterizuje bezpečnost informací a její organizační zabezpečení. Definuje související pojmy a legislativní vymezení řešené problematiky. Praktická část úvodem definuje systém zdravotnictví v České republice, dále podrobně popisuje zdravotnickou dokumentaci jako hlavní zdroj citlivých údajů a popisuje zákonné normy, kterými se zdravotnická zařízení musí řídit. Další část se již zaměřuje na analýzu rizik, zahrnující komplexní posouzení bezpečnostní politiky v organizaci. Závěr práce je věnován vyhodnocení analýzy a jsou navrženy opatření ke snížení definovaných rizik.

Klíčová slova: bezpečnost, riziko, informace, zdravotnictví, analýza rizik,

ABSTRACT

My thesis deals with difficulties in protection of sensitive information of patients in public health services. Theoretic part defines basic terms connected with data protection and describes data security management. It also circumscribe other relevant terms and general legal issues connected with this topic. Practical part starts with a description of health system in Czech Republic. In the next part there is a detailed description of medical records and it is characterized as a main source of sensitive information. This part interprets the legislation for data protection in medical facilities. Following part offers risk assessment analysis and involves detailed summary of policies practised in the organization. Finally my thesis sums up the results of my analysis and there are offered steps that could lead to degradation of defined risks.

Keywords: safety, risk, information, health system, risk analysis

Chtěla bych poděkovat hlavně svému synovi za motivaci a podporu při studiu. Mé poděkování patří také přátelům a spolupracovníkům za trpělivost a cenné rady nejen při zpracování bakalářské práce, ale v průběhu celého studia.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Ochrana osobních údajů je v dnešní době, a to nejen díky rozvoji informačních technologií, velmi diskutované téma. Zvolené téma „ Informační bezpečnost a její organizační zabezpečení“ je zaměřené na oblast zdravotnictví, jelikož ji lze považovat z pohledu zpracování osobních údajů a jejich ochrany, za jedno z nejnáročnějších odvětví.

Po úvodu do řešené problematiky, který obsahuje vymezení základních pojmů, právní rámec bezpečnosti informací, je teoretická část věnována již samotné bezpečnosti osobních údajů, vývoji legislativy a uvedení způsobů nakládání s těmito údaji. Kapitola s názvem informační bezpečnost, popisuje jednotlivé prvky informační bezpečnosti, úrovně a způsoby opatření. Poslední kapitola teoretické části se věnuje organizačnímu zabezpečení informací, které zahrnuje analýzu, implementaci protiopatření a závěrečně kontrolní audit.

Praktická část začíná všeobecnou specifikací zdravotnických zařízení. Popisuje soustavu zdravotnických zařízení v České republice, kdo je jejich zřizovatelem a jaké jsou druhy zdravotní péče. Následuje kapitola o zdravotnické dokumentaci, jako hlavnímu zdroji citlivých údajů pacientů, v níž je uvedeno, co je obsahem dokumentace, jaké jsou povinnosti správců údajů, kdo zdravotnickou dokumentaci vlastní, způsoby nahlížení do dokumentace a v neposlední řadě také zásady vyřazování a skartace zdravotnické dokumentace. Samozřejmostí je uvedení legislativy týkající se problematiky ochrany informací ve zdravotnictví, které je věnována také jedna z kapitol. Následuje popis konkrétního zdravotnického zařízení, ve kterém je výše uvedená problematika řešena a následně je provedena analýza rizik, která začíná popisem stávající situace v organizaci. Poté jsou definována a vyhodnocena rizika s návrhy na jejich snížení.

Ke zjištění rizik v organizaci byl úvodem realizován vlastní průzkum v organizaci. Dále hodnocení rizik probíhalo metodou What-if, formou brainstormingu a následných cílených rozhovorů s náhodně vybranými zaměstnanci organizace. Definovaná rizika jsou okomentována a ohodnocena skórovací metodou a znázorněna na mapě rizik. Následují doporučení vedoucí k odstranění definovaných rizik.

Cílem práce je vytvoření uceleného přehledu problematiky týkající se ochrany a zabezpečení informací, která se následně v praktické části zaměřuje na zdravotnictví.

I. TEORETICKÁ ČÁST

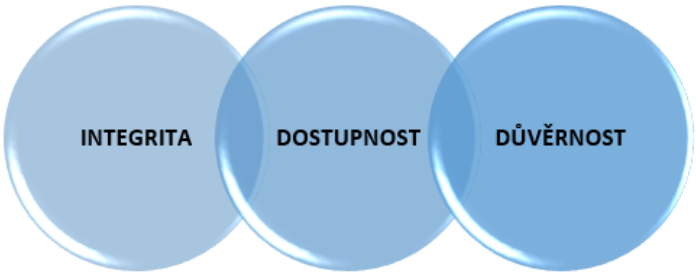
1 ÚVOD DO PROBLEMATIKY

Hodnotu informací si organizace často neuvědomují nebo si ji uvědomí až v okamžiku, kdy už je pozdě. Důsledky ztrát informací mohou vést ke ztrátě dobrého jména, důvěry klientů nebo i k zániku společnosti. Organizace, které si dnes uvědomují hodnotu informací, vynakládají nemalé finanční prostředky na zajištění jejich bezpečnosti. [1]

Informace, které je třeba chránit, mají rozličnou podobu a to od té elektronické, přes tištěnou až třeba po informace, které se dají vypozorovat z logických procesů či rozmístění pracovišť. Rizika úniku a zneužití informací hrozí nejen z vnějšího prostředí, ale zejména zevnitř. **Lidský faktor je nejčastější slabou stránkou bezpečnostních systémů**. [2]

Kromě pojmu informace, který je podrobně objasněn v následující kapitole, se setkáváme při práci s informacemi a jejich ochraně i s dalšími pojmy. Mezi ně neodmyslitelně patří **bezpečnost informací.**

Bezpečnost je obecně chápána jako ochrana něčeho před zničením, poškozením nebo ztrátou. V případě bezpečnosti informací hovoříme o zachování jejich **důvěrnosti**, **integrity** a **dostupnosti**. Vzájemný vztah těchto tří bezpečnostních atributů je znázorněn na následujícím obrázku (Obr. 1). [1]

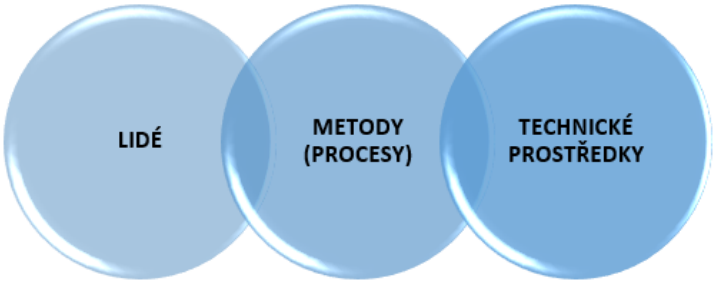


Obr. 1 Vztah bezpečnostních prvků. [1]

- **Dostupnost** můžeme definovat jako vlastnost, že informace je pro osobu, která je oprávněna se s ní seznamovat, k dispozici v okamžiku, kdy s ní potřebuje pracovat.
- **Důvěrnost** znamená, že s informacemi se mohou seznamovat pouze oprávněné osoby.
- Zachování **integrity** spočívá v tom, že informaci můžeme důvěřovat a spolehnout se na to, že nebyla pozměněna. [1]

Další pojem, se kterým se při práci s informacemi setkáme, je **informační systém.**

Od počátku aktivit organizace je třeba mít pořádek ve spisové obchodní, ekonomické, finanční a ostatní agendě. Musíme mít jistotu, že žádný dokument, dopis či spis a v nich uložené informace se neztratí. Proto je nezbytné si na základě druhu činnosti vytvořit informační systém a současně rozhodnout za pomocí jakých prostředků ho budeme uskutečňovat. Zejména po zavedení výpočetní techniky, je tento předpoklad efektivní práce nezbytný. Informační systém je tedy **soubor lidí** (zdrojů, zpracovatelů, uživatelů), **technických prostředků** a **metod**, zabezpečující sběr, přenos, uchování a zpracování dat za účelem tvorby a prezentace informací pro potřeby uživatelů. Prvky informační bezpečnosti jsou znázorněny na následujícím obrázku (Obr. 2). [2]

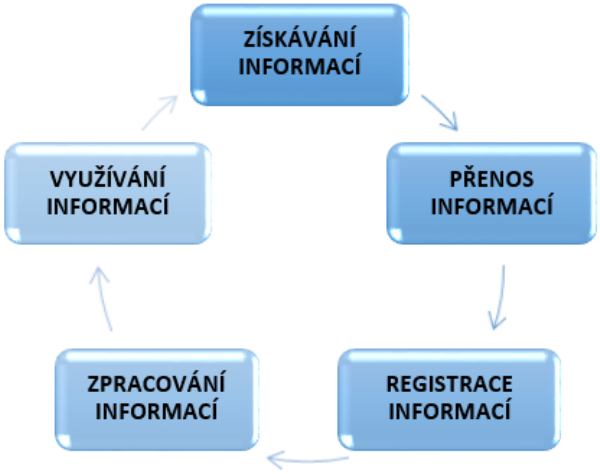


Obr. 2 Prvky informačního systému. [2]

Provádění určitých činností s informacemi se označuje jako **informační proces.**

Jedná se o uzavřený cyklus (Obr. 3), kterým informace prochází od svého vzniku až ke svému užití. Je zabezpečený vhodným informačním systémem jako je sled operací s daty a informacemi, který zejména obsahuje tyto kroky:

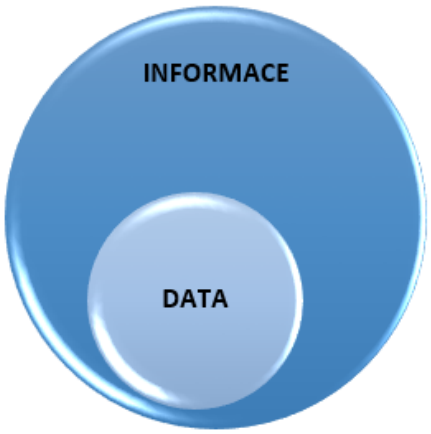
- získávání (sběr informací);
- přenos informací od zdroje k místu zpracování a jejich soustřeďování;
- registraci (evidování) na místě zpracování;
- zpracování informací (třídění, vyhledávání, analýza);
- využívání informací. [2]



Obr. 3 Informační proces. [2]

1.1 Klasifikace informací

Pojem informace patří k nejobecnějším kategoriím současné vědy. Podle toho, ve kterém vědním oboru či lidské činnosti se používá, jsou různé způsoby jejího chápání a definování. Pojmy data a informace se v praxi často zaměňují nebo slučují. Data jsou většinou chápána jako statistická fakta, časově nezávislá. Smyslem zpracování dat je vytvoření informace. Informace je význam přisouzený datům a odrážejí stav v určitém okamžiku, a proto je nelze měnit (Obr. 4). [2]



Obr. 4 Vzájemný vztah dat a informací. [2]

Informace je možné členit na **veřejné informace**, to jsou informace, které jsou přístupné pro čtení komukoliv. Přechodovým stavem, z pohledu jejich ochrany, jsou informace, které nejsou úplně veřejné, ale na které se nevztahují žádné další zákonné normy z pohledu jejich ochrany. Ty jsou nazývány **informacemi neveřejnými**. V organizaci se může jednat například o informace provozního charakteru. Ostatní informace, respektive práce s nimi, je nějakým způsobem regulována.

První velkou skupinou, která patří mezi regulované informace, jsou **informace citlivé**. Tato kategorie se pak dělí na informace:

- **důvěrné** – osobní údaje, obchodní tajemství a informace smluvní strany;
- **přísně důvěrné** – citlivé (osobní) údaje.

Poslední skupinou, se kterou se můžeme v praxi setkat, jsou informace **utajované**. Utajované informace rozdělujeme do čtyř stupňů utajení. Jedná se o stupně:

- **vyhrazené**
- **důvěrné**
- **tajné**
- **přísně tajné** [3]

Kromě uvedené klasifikace existují ještě i další klasifikace informací, se kterými se můžeme v praxi setkat. Jedná se o klasifikace Evropské unie nebo klasifikace NATO. Tyto klasifikace většinou odpovídají klasifikaci utajovaných informací. Zajímavou kategorií z hlediska zajištění bezpečnosti informací je kategorie tzv. „**Zvláštní skutečnosti**“. Jedná se o informace chráněné podle ustanovení zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů. V podstatě se jedná o informace přísně důvěrné, které mají vztah k výkonu státní správy v krizových situacích. [3]

1.2 Právní rámec bezpečnosti informací

Součástí informační společnosti a prosazování ochrany užívání informačních systémů a informačních a komunikačních technologií je v každé společnosti spojeno s přijetím odpovídajících zákonů a se zřízením příslušných institucí. Nasazováním informačních technologií do plošného užívání nejen v komerční sféře, ale i pro potřeby veřejné a státní správy představuje obrovský nárůst objemu uchovávaných dat, z nichž mnohá mají takový charakter, že jejich zveřejnění by mohlo významným způsobem poškodit zainteresované osoby.

Prvním krokem pro řešení otázek bezpečnosti při práci s elektronickou formou dat je modifikace stávajícího právního řádu, tj. přijetí nových nebo úpravy již existujících zákonů. Tyto zákony upravují způsob pořizování dat, jejich uchovávání a zpracování v podmínkách nasazení informačních a komunikačních technologií. Mnohé zákony přímo ukládají povinnosti různým institucím nebo právním subjektům. Dalším úkolem nově vzniklých zákonů je harmonizovat právní řád České republiky s právními řády ostatních členských států Evropské unie. [3]

Níže jsou uvedeny některé důležité vybrané zákonné normy České republiky, které mají vliv na problematiku bezpečnosti informací.

- Zákon České národní rady č. 20/1993 Sb., o zabezpečení výkonu státní správy v oblasti technické normalizace, metrologie a státního zkušebnictví;
- Zákon č. 106/1999 Sb., o svobodném přístupu k informacím;
- Zákon č. 29/2000 Sb., o poštovních službách;
- Zákon č. 101/2000 Sb., o ochraně osobních údajů;
- Zákon č. 121/2000 Sb., autorský zákon;
- Zákon č. 151/2000 Sb., o telekomunikacích;
- Zákon č. 227/2000 Sb., o elektronickém podpisu;
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy;
- Vyhláška č. 496/2004 Sb., o elektronických podatelnách;
- Zákon č. 499/2004 Sb., o archivnictví a spisové službě;
- Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů;
- Zákon č. 111/2009 Sb., o základních registrech;
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti. [3]

1.3 Organizace zabývající se bezpečností informací

Na základě některých výše uvedených zákonů byly zřízeny instituce, jejichž hlavním úkolem je řešit otázky, spojené s bezpečností informačních systémů a informačních a komunikačních technologií převážně řídícího a kontrolního charakteru. Instituce se zaměřují na vybrané oblasti bezpečnosti informací, stanovují bezpečnostní požadavky.

Přehled organizací, které se zabývají bezpečností informací:

- Úřad pro ochranu osobních údajů;
- Národní bezpečnostní úřad;
- Ministerstvo vnitra, Odbor koncepce a koordinace;
- Český normalizační institut;
- Úřad pro technickou normalizaci, metrologii a státní zkušebnictví;
- Český institut pro akreditaci;
- Český telekomunikační úřad. [3]

2 BEZPEČNOST OSOBNÍCH ÚDAJŮ

Z velkého množství informací a údajů, se kterými se v rámci fungování jakékoliv organizace setkáváme, se podrobněji zaměřím **osobní (citlivé) údaje** a následně v praktické části práce na jejich ochranu. Tato problematika je řešena především zákonem:

- **č. 101/2000 Sb., o ochraně osobních údajů** (ZOOÚ)**.**

2.1 Vymezení základních pojmů

Osobní údaj

První z pojmů ochrany osobních údajů vyžadující logickou i právní interpretaci je **osobní údaj**. Je definován v ZOOÚ v § 4 písm. a), a to poměrně stručně a jednoduše jako jakákoliv informace, která se týká konkrétního subjektu údajů. Definice užitá v zákoně se omezuje na vymezení vztahu údaje k tomu, o kom vypovídá, tj. subjektem údajů. Z tohoto úhlu pohledu a při aplikaci zákona v praxi vyjadřuje osobní údaj vždy vztah mezi reálnou fyzickou osobou a hodnotou údaje. [4]

Citlivý osobní údaj

Mezi osobními údaji zaujímající specifické postavení, jsou **citlivé osobní údaje**, jejichž nekorektní užití může mít pro subjekt údajů zvláště závažné důsledky. Na základě zpracování těchto údajů může docházet k porušování základních lidských práv. Proto jsou citlivé osobní údaje přesně definovanou kategorií a pro jejich zpracování ukládá jak příslušná evropská směrnice 95/46/ES v článku 8, tak český ZOOÚ v § 9 přísnější režim než pro ostatní údaje. Citlivý je údaj, který může být použit k diskriminaci subjektu údajů bez vazby na hodnoty dalších osobních údajů téhož subjektu údajů. Citlivými údaji jsou: zdravotní stav, jedinečné biologické rysy (otisk prstu, obraz sítnice, genetická charakteristika), původ národnostní, rasový, etnický, sexuální orientace, odsouzení za trestný čin, politické postoje, členství v odborných organizacích, údaje vypovídající o náboženství, politických postojích a filosofickém přesvědčení. [4]

Kým mohou být citlivé údaje nejspíše zneužitelné, je dáno tím, o jaký údaj se jedná a v jakém prostředí se pohybuje subjekt údajů. Jsou situace, které vytvářejí předpoklady pro využití údajů, přinášejí někomu diskriminaci, i když ten, kdo diskriminuje, sleduje primár-

ně vlastní, nezřídka ekonomický prospěch. V takových situacích může být zájem zpracovávat údaje vypovídající např. o zdravotním stavu nebo o odsouzení za trestný čin. Využitelnost těchto údajů v neprospěch subjektu údajů je nicméně absolutní, a proto jsou na nakládání s nimi uvaleny výrazně přísnější podmínky než na nakládání se všemi ostatními osobními údaji. Právě u nich platí bez výjimky poučka, že nejlepší ochranou je takové údaje nepoužívat. [4]

Subjekt údajů

Dalším pojmem k objasnění je **subjekt údajů**. Tímto subjektem může být výlučně fyzická osoba, ke které se osobní údaje vztahují. Není rozhodné, zda se jedná o občana České republiky nebo o cizince, důležitý není její věk, skutečnost, zda má zachovanou plnou způsobilost k právním úkonům apod. Subjektem údajů zásadně nemůže být právnická osoba, u níž pojmově vůbec nelze o osobních údajích hovořit. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků. [5]

Správce

Další mezi často používané pojmy v ZOOÚ patří pojem **správce**. Ten je ústředním nositelem povinností při zpracovávání osobních údajů. Je jím každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí samotné zpracování a odpovídá za něj. Má také možnost tímto zpracováním pověřit nebo zmocnit tzv. zpracovatele, pokud zvláštní zákon nestanoví jinak. Pro správce je tedy stanovena odpovědnost za samotné zpracování osobních údajů. Za dodržování povinností stanovených ZOOÚ je však odpovědný jak správce, tak zpracovatel, popřípadě i jiné osoby, které vykonávají činnost při zpracování osobních údajů pro správce nebo zpracovatele na základě smlouvy. Účel, pro který budou údaje zpracovávány správcem, může vyplývat přímo ze zvláštního zákona, na jehož základě bude ke zpracování docházet, ale je zde také možnost, aby si správce určil účel zpracování sám. Jednotlivými správci jsou například ústřední správní úřady, jiné správní úřady, obce nebo také soudy. Dále správcem může být zaměstnavatel zpracovávající údaje o svých zaměstnancích. [5]

Správce je při shromažďování osobních údajů povinen subjekt údajů informovat o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny, nejsou-li subjektu údajů tyto informace již známy. Správce musí subjekt údajů informovat o jeho právu přístupu k osobním údajům, právu na opravu osobních údajů, jakož i o dalších právech stanovených v § 21 příslušného zákona. [6]

Zpracovatel údajů

S pojmem správce údajů úzce souvisí pojem **zpracovatel údajů**. Tímto zpracovatelem je každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle ZOOÚ. Zpracovatel, na rozdíl od správce, neurčuje účel ani prostředky zpracování osobních údajů. Zpracovatelem se rozumí také jakýkoli jiný subjekt, který provádí jen některou činnost (nebo některé činnosti) související se zpracováním. Nemusí tedy jít vždy o subjekt, který osobní údaje shromáždil. [6]

2.2 Vývoj legislativy ochrany osobních údajů

První právní předpisy k ochraně osobních údajů vznikly v 70. letech 20. století. Řada lidí otevřeně a upřímně prohlašuje, že jim na osobních údajích nezáleží a že nakládání s nimi někým jim nevadí. Jiní lidé se naopak snaží nalézt v právní ochraně osobních údajů pomoc a oporu při řešení prakticky jakéhokoli problému ve styku s reprezentací libovolné institucionalizované moci. Zvláštní zákony o ochraně osobních údajů vznikají jako reakce na možnosti jednotlivce ovlivnit využívání osobních údajů o sobě samém. Proto jim musí zákony poskytnout určité záruky a jistou ochranu. [7]

Ochrana osobních údajů, tak jak je dnes zakotvena v právním řádu České republiky a prakticky všech států, na něž se Česká republika politicky orientuje, a mezinárodních organizací, si neklade za cíl absolutně bránit používání osobních údajů jiných lidí. Jejím jediným deklarovaným a s větším či menším úspěchem naplňovaným cílem je zabránit zneužití osobních údajů a zároveň umožnit zpřístupnění osobních údajů k legálním účelům. [4]

Prvním mezinárodně platným právním dokumentem dopadajícím specificky na problematiku ochrany osobních údajů je specificky zaměřená **Úmluva č. 108** o ochraně osob se zře-

telem na automatizované zpracování osobních údajů, která byla otevřena k podpisu 28. 1. 1981. Úmluva vstoupila v platnost v roce 1985 poté, co ji ratifikovalo prvních 5 členských států Rady Evropy (Švédsko, Francie, Norsko, Španělsko a Spolková republika Německo). Její význam spočívá zejména ve formulaci základních zásad ochrany osobních údajů. V roce 2001 byl přijat Dodatkový protokol o orgánech dozoru a o toku údajů přes hranice. Česká republika Úmluvu ratifikovala dne 9. 7. 2001 s účinností ode dne 1. 11. 2001, resp. Dodatkový protokol dne 21. 9. 2003 s účinností ode dne 1. 7. 2004. [8]

Úmluva vymezila základní **pojmy** (např. pojem osobní údaj) a **zásady** (např. poctivý a právně zajištěný sběr a zpracování osobních údajů, shromažďování osobních údajů jen pro vymezené legitimní účely, znemožnění zpracování údajů k jiným účelům, než pro které byly shromážděny, časové omezení zpracování údajů po naplnění stanoveného účelu atd.). Touto Úmluvou byly rovněž stanoveny i požadavky, které při zpracování údajů musí být splněny a upraveno je také předávání údajů do zahraničí. [9]

Účelem této Úmluvy je zaručit na území každé smluvní strany každé fyzické osobě, úctu k jejím právům a základním svobodám, a zejména k jejímu právu na soukromý život, se zřetelem k automatizovanému zpracování osobních údajů, které se k ní vztahují. [4]

Pro oblast Evropské unie byla dne 24. října 1995 přijata zvláštní **Směrnice 95/46/ES**, o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a s volným pohybem těchto údajů. Jelikož se jednalo o směrnici, musela se jí přizpůsobit právní úprava členských států. Touto směrnicí tedy bylo uloženo členským státům, že mají do tří let uvést svoje právní řády do souladu s jejím obsahem. Přizpůsobovaly se i právní řády států, které se teprve ucházely o členství v Evropské unii. Takovým státem byla i ČR, která v roce 1996 podala oficiálně žádost o vstup ČR do Evropské unie a předala potřebné podklady pro posouzení své připravenosti k vstupu. Jedním z okruhů, které jsou předmětem posuzování, je i nakládání s osobními údaji, resp. ochrana osobních údajů. [5]

Směrnice 95/46/ ES byla do právního řádu České republiky implementována **ZOOÚ**, který nabyl účinnosti 1. června 2000. Tento nástupce zákona č. 256/1992 Sb. o ochraně osobních údajů v informačních systémech, zahrnul do své úpravy ochranu jak automatizovaných údajů, tak i údajů zpracovávaných manuálně. Stanovil informační povinnost tomu, kdo s údaji nakládá vůči osobě, které se údaje týkají. Došlo k upřesnění práva na opravu nesprávných a neaktuálních údajů. Podrobně byl vymezen rozsah citlivých údajů a upuštěno

bylo od používání neurčitých a hlavně špatně definovatelných pojmů jako „soukromí a osobnost dotčené osoby“, „majetkové poměry“. Velkým přínosem byl vznik **ÚOOÚ** jako kontrolního orgánu nadaného dozorovými a registračními pravomocemi.

Kromě uvedené směrnice byly tímto zákonem do českého právního řádu zahrnuty principy ochrany osobních údajů vycházející z Úmluvy č. 108, kterou Česká republika ratifikovala krátce poté, co ZOOÚ nabyl účinnosti. [5]

2.3 Nakládání s údaji

Lze zpracovávat jen osobní údaje, které jsou **pravdivé a přesné**. Je možné s nimi nakládat jen k předem stanovenému účelu a v nezbytně nutném rozsahu. Údaje se uchovávají jen po dobu nezbytně nutnou a k naplnění stanoveného účelu. Pokud zpracování dat nestanoví zákon, je k tomu nezbytný náš jednoznačný souhlas. To znamená souhlas se zpracováním každého údaje. V případě **citlivých údajů** zákon stanoví náš **výslovný souhlas**. Nesouhlas je naopak nutné uvést písemnou formou. Ten kdo souhlas vyžaduje, musí při kontrole úřadu prokázat, že jej od nás získal.

Máme právo vědět, kdo, jaké naše osobní údaje a za jakým účelem je zpracovává, zda mohou být předány jinému subjektu a jak dlouho je bude uchovávat. Pokud zjistíme, že naše údaje jsou zpracovávány v chybné podobě, máme právo se dožadovat jejich upřesnění, případně výmazu. Omezení těchto práv může být stanoveno pouze zákonem. Porušení zákonných práv hlásíme ÚOOÚ. [10]

Při nakládání s osobními údaji, které je v rozporu se zákonem, se mohou fyzické osoby dopustit přestupku případně trestného činu a právnické osoby a fyzické osoby podnikající jiného správního deliktu. Přestupky nebo trestné činy nejsou jenom doménou správce nebo zpracovatele osobních údajů, ale kohokoli, kdo s osobními údaji nějak nakládá. Správce a zpracovatel se však mohou právně závadných jednání dopustit poměrně častěji než „nesprávci“, neboť musí plnit mnohem více povinností. [11]

Jelikož je při nezákonném nakládání s osobními údaji porušeno právo na ochranu osobnosti člověka, jež chrání podstatné atributy lidské existence jako je např. soukromí, důstojnost, čest apod., jejichž náprava je obtížná, ne-li nemožná, jsou sankce za porušování povinností při nakládání s osobními údaji stanoveny poměrně přísně (např. ve srovnání s neplacením daní). Přestupky a správní delikty jsou stanoveny v ZOOÚ. [11]

3 INFORMAČNÍ BEZPEČNOST

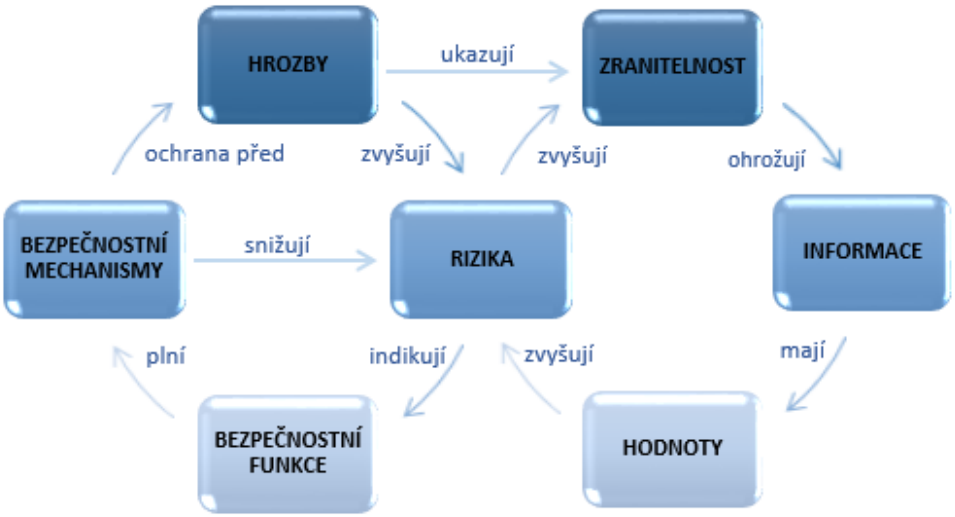
Informační bezpečnost představuje ochranu informace před širokým spektrem možných hrozeb ve všech jejich formách a po celý její životní cyklus. Tato ochrana tedy pokrývá část vzniku, zpracování, přenosu, uchování a samozřejmě i likvidaci či znehodnocení informace. Z pohledu informační bezpečnosti jsou informace chráněny bez ohledu na jejich umístění a formu. Mohou tedy být umístěny v informačním systému, vytištěné na papíře nebo mohou být předávány ústně.

S informacemi může být nakládáno různým způsobem. Pro jejich ochranu je důležité si stanovit několik základních otázek: Co chránit? Proč informaci chránit? Kdy chránit? Proti jakým hrozbám informaci chránit? Jakým způsobem informaci chránit? [2]

3.1 Prvky informační bezpečnosti

Základní koncept zajištění bezpečnosti představuje vztahy mezi **aktivy** organizace, **hrozbami**, které na ně mohou potenciálně působit, možnou **zranitelností** aktiv reálnými hrozbami, **dopady** reálných hrozeb na tato aktiva a možnostmi **ochrany** aktiv organizace formou protiopatření. [2]

Schéma (Obr. 5) zachycuje, jakým způsobem jsou ovlivněny všechny **prvky informační bezpečnosti**. Tzn., čím jsou bezpečnostní rizika posilovány či naopak oslabovány. [2]



Obr. 5 Prvky informační bezpečnosti. [16]

Mezi prvky informační bezpečnosti patří:

Aktivum

Aktiva jsou všechny hmotné i nehmotné statky, vše co má pro majitele informačního systému hodnotu. Za nejcennější aktiva se považují především data a informace, jejichž zneužití, ztráta nebo modifikace by organizaci nebo osobě způsobily škodu. [2]

Aktivy v oblasti informačního systému z pohledu věcného rozumíme především:

- **hmotná aktiva** patří zde především technické prostředky výpočetní techniky – počítače, modemy, tiskárny a ostatní technická zařízení;
- **nehmotná aktiva** jsou pracovní postupy využívané v organizaci, data vytvořené organizací, které jsou důležité pro její provoz. Dále programové vybavení (např. operační systémy a programové vybavení počítačů), aplikační programové vybavení (např. textové editory, grafické programy), služby (počítačové a komunikační služby) a také základní služby potřebné k zajištění provozu (např. světlo, topení, klimatizace). [3]

Hrozba

Je skutečnost, událost, síla nebo osoby, jejichž působení může způsobit poškození, zničení, ztrátu důvěry nebo hodnoty aktiva. Hrozba může ohrozit bezpečnost (např. přírodní katastrofa, hacker, zaměstnanec aj.). [2]

Hrozby rozdělujeme zejména na:

- **přírodní a fyzické**, což jsou živelné pohromy a nehody, jako jsou např. požáry, povodně, poruchy v dodávce elektrického proudu;
- **technické a technologické,** které zahrnují poruchy nosičů dat, poruchy sítí, poruchy způsobené programy (nesprávná funkčnost – např. nedostatečně otestované programové vybavení, viry);
- **lidské** a to jak neúmyslné, které vyplývají z neznalosti nebo zanedbání plnění povinností, tak úmyslné, které dále rozdělujeme na působící zvenku systému (hackeři, teroristé, mezifiremní špionáž apod.) a působící zevnitř organizace, to jsou většinou zlomyslní, chamtiví zaměstnanci, hosté a návštěvníci organizace.

Převážná většina hrozeb, které poškodí informační systém organizace (více než 50 % ze všech), patří do kategorie neúmyslných hrozeb. Také podíl hrozeb zevnitř organizace je významně vyšší než hrozby z vnějšku. Podle některých statistických zdrojů až 98 % všech bezpečnostních incidentů v organizaci je interního původu. Většinou nedbalost pracovníků, která je nejčastěji způsobena jejich neznalostí problematiky bezpečnosti informačních systémů. [3]

Riziko

Riziko je pravděpodobnost, s jakou bude daná hodnota aktiva zničena nebo poškozena působením konkrétní hrozby, která působí na slabou stránku této hodnoty. Je to tedy míra ohrožení konkrétního aktiva. [3]

Opatření

Opatření rozdělujeme na ta, jež mají charakter:

- **administrativní**, zejména různé směrnice pro práci s informačním systémem v organizaci;
- **fyzický**, jako je např. používání zámků, čipové karty pro přístup do tzv. režimových prostorů;
- **technický a technologický**, např. autorizace a autentizace přístupu uživatelů k aktivům informačního systému, které se projevují ochranou přístupů do informačního systému prostřednictvím hesel. [3]

Opatření sledují následující cíle: **prevenční** (zajištění minimalizace rizik předem), jedná se např. o odhlášení uživatele při jeho nečinnosti delší než určitou dobu, automatické uzavírání dveří, **detekční** (odhalování potencionálních problémů a hrozeb), např. pravidelné vyhodnocování auditních záznamů s možností identifikace bezpečnostních incidentů a **korekční** (minimalizace dopadů poté co hrozba nastala a projevila se), jde o odstranění virů z napadených souborů.

Jako příklad **opatření** lze uvést vhodné umístění budov a místností, uzamykání objektů, používání hesel při přístupu k systému při procesu autentizace, užití homologovaných a schválených zařízení aj. [3]

Útok

Útok, který nazýváme rovněž bezpečnostní incident, rozumíme využití zranitelného místa ke způsobení škod či ztrát na aktivech informačního systému, nebo neúmyslné uskutečnění akce, jejímž výsledkem je škoda na aktivech. [3]

Zranitelnost

Zranitelnost je nedostatek nebo slabina bezpečnostního systému, která může být zneužita hrozbou tak, že dojde k poškození nebo zničení hodnoty aktiv. Každé aktivum je zranitelné, protože jeho hodnotu ohrožují různé vlivy. [2]

Zranitelnost rozdělujeme na

- **fyzickou** zahrnující budovy a počítačové místnosti, tedy oblast působnosti bezpečnosti organizace;
- **technických a programových prostředků,** která se projevuje chybou či poruchou.

Dalším slabým místem jsou:

- **nosiče dat** jsou dalším slabým místem (např. selhání nosiče), elektromagnetické zařízení, komunikační systémy a kabelové rozvody, kdy může dojít k přerušení nebo i možným odposlechům;
- **zranitelnost personální**, která plyne z úmyslného či neúmyslného chování osob, jejich přirozených chyb. [3]

Zranitelné místo

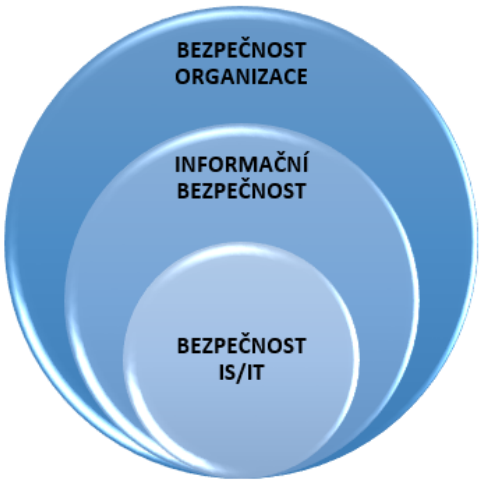
Slabinu informačního systému využitelnou ke způsobení škod nebo ztrát útokem na informační systém nazýváme zranitelné místo. Existence těchto míst je důsledek chyb, selhání v analýze, v návrhu nebo implementaci informačního systému. [2]

Dopady hrozeb na aktiva mohou mít různorodý charakter. Od okamžitého efektu ve formě bezprostřední **finanční ztráty** (např. zničení počítače) až po efekty, které nejsou na první pohled zřejmé a objevují se postupně (např. ztráta dobré pověsti organizace nebo pravidelný únik informací z ní). Dopady všech hrozeb se převádějí na finanční hodnoty. [3]

3.2 Úrovně bezpečnosti informací

Vývoj bezpečnosti informací a jejího systému řízení nemá příliš dlouhou tradici. Jeho intenzivní potřeba začala vznikat v době, kdy se lokální počítače začaly propojovat do počítačových sítí a významněji se rozšířily komunikační kanály mezi počítači různých právních subjektů a organizací.

V souvislosti s termínem bezpečnosti informací je nutné se zmínit ještě o dalších dvou pojmech (Obr. 6) a to **bezpečnost organizace** a **bezpečnost informačních systémů a informačních a komunikačních technologií** (bezpečnost IS/IT). [3]



Obr. 6 Vztah úrovní bezpečnosti. [3]

Kategorie bezpečností v organizaci:

- **Bezpečnost organizace**. Její součástí je zajištění bezpečnosti objektů, majetku organizace, jako je ostraha přístupů do objektů, strážní služba apod. Některé její činnosti napomáhají zároveň i zajištění bezpečnosti informačního systému jako např. kontrola oprávnění fyzického přístupu do budov. Její součástí je i informační bezpečnost.
- **Informační bezpečnost** zahrnuje navíc proti bezpečnosti informačních systémů a informačních a komunikačních technologií i způsob zpracování, uložení a správy archivu nedigitálních dat, zásady skartace materiálů, nakládání s informacemi během jejich transportu, zásady pro poskytování informací apod. [3]

- **Informačních systémů a informačních a komunikačních technologií** má za úkol chránit pouze ta aktiva, která jsou součástí informačního systému organizace. Proto je tato bezpečnost relativně nejužší oblastí řízení bezpečnosti. [3]

3.3 Informační bezpečnost a kybernetický zákon

Kybernetická bezpečnost je pojem 21. století, který velmi úzce souvisí s rozvojem informačních technologií a internetovým pojetím společnosti. Jedná se o určitý soubor povinností, zásad a pravidel, která by měla být závazná pro každého uživatele či provozovatele informačních technologií. Gestorem oblasti kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast je v České republice Národní bezpečnostní úřad (NBÚ). **Zákon o kybernetické bezpečnosti č. 181/2014 Sb.,** nabyl platnost 1. ledna 2015. V souvislosti s touto problematikou je dobré připomenout, že i Trestní zákoník zná trestné činy související s neoprávněnými přístupy do informačních systémů, konkrétně § 230 nazvaný „Neoprávněný přístup k počítačovému systému a nosiči informací“. Také nový Občanský zákoník pamatuje na škodu způsobenou informací nebo radou. [12]

Výše uvedený zákon o kybernetické bezpečnosti se vztahuje na:

- **poskytovatele služeb elektronických komunikací** (poskytovatel internetového připojení). Ti mají podle zákona povinnost nahlásit kontaktní údaje a v případě kybernetického nebezpečí provádět opatření vydaná NBÚ);
- **významné sítě** (jedná se o síť elektronických komunikací zajišťující přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťující přímé připojení ke kritické informační infrastruktuře. Vztahují se na ně stejná pravidla jako na poskytovatele);
- **informační a komunikační systémy kritické informační infrastruktury** (tyto prvky definuje vyhláška č. 315/2014 Sb., z nejrůznějších odvětví, např. energetiky, zdravotnictví, dopravy, komunikace atd. Pro tyto systémy je již povinností podstatně více. Stejně jako poskytovatelé musí nahlásit kontaktní údaje a provádět opatření vydaná NBÚ. Kromě toho na sebe musí brát i aktivní roli, která spočívá v detekci, dokumentaci a hlášení kybernetických bezpečnostních incidentů);

- **významné informační systémy** (kategorie vyhrazena pro systémy orgánů veřejné moci. Jsou přímo vyjmenované ve vyhlášce č. 317/2015 Sb. Aktuálně je jich celkem 92 a jedná se o nejrůznější systémy ministerstev a významných úřadů. Například Centrální registr vozidel, Registr živnostenského podnikání nebo Centrální registr pojištěnců. Platí zde stejné povinnosti jako v předchozím bodě). [13]

Povinnost plynoucí ze Zákona o kybernetické bezpečnosti se dotýkají jen vymezeného okruhu právnických osob, orgánů a podnikajících fyzických osob. To ale neznamená, že ostatních subjektů se potřeba chránit své informační systémy před narůstajícími kybernetickými hrozbami nijak netýká. [14]

3.4 Informační vs. kybernetická bezpečnost

V poslední době se dost často hovoří o kybernetické bezpečnosti a zapomíná se, že existuje i informační bezpečnost. Je kybernetická bezpečnost a informační bezpečnost totéž? Je jedna bezpečnost podmnožinou té druhé nebo mezi nimi dochází k určitému průniku? Na schématu (Obr. 7) je zachycen vztah mezi zmiňovanými bezpečnostmi. [15]

Obr. 7 Vztah bezpečností. [15]

Z obrázku vyplývá, že kybernetická bezpečnost je podmnožinou informační bezpečnosti. A to z toho důvodu, že cílem informační bezpečnosti je ochrana informací v jakékoliv podobě, zatímco cílem kybernetické bezpečnosti je ochrana dat pouze v digitální podobě. [15]

3.5 Realizace bezpečnostních opatření

Základním východiskem řízení bezpečnosti informací je norma **ISO/IEC 27002:2005 – soubor pro řízení bezpečnosti informací.** Norma obsahuje 153 bezpečnostních opatření, která jsou rozdělena do jedenácti oblastí (Obr. 8) [3]

Obr. 8 Oblasti bezpečnosti informací. [3]

Jednotlivé oblasti zahrnují:

- **Bezpečnostní politika** definuje základní pravidla bezpečnosti informací a vyjadřuje podporu vedením organizace.
- **Řízení aktiv** představuje udržování přehledu o existujících aktivech organizace a stanovení odpovědnosti za udržování přiměřené míry ochrany jednotlivých aktiv.
- **Řízení přístupu** obsahuje pravidla pro přidělování přístupu ke všem prostředkům informačních a komunikačních systémů včetně sledování způsobu využívání dostupných prostředků.
- **Organizace bezpečnosti informací** upřesňuje struktury pro řízení informací uvnitř organizace a řízení bezpečnosti ve vztahu k externím subjektům (zákazníkům, dodavatelům).
- **Bezpečnost z hlediska lidských zdrojů** vymezuje povinnosti na ochranu informací u všech pracovníků a zajištění potřebného bezpečnostního povědomí. [3]

- **Fyzická bezpečnost a bezpečnostní prostředí** definuje pravidla pro přístup osob do klíčových prostor organizace a ochrana zařízení, zejména zařízení informační technologie.
- **Řízení komunikací a řízení provozu** zajišťuje spolehlivý a bezpečný chod produkčních informačních a komunikačních systémů organizace.
- **Akvizice, vývoj a údržba informačních systémů** prosazuje principy bezpečnosti informací do projektů rozvoje informačních technologií a dalších podpůrných aktivit.
- **Řízení kontinuity činností organizace** zahrnuje postupy prevence a minimalizace škod plynoucích z havárií, živelných pohrom či jiných mimořádných událostí.
- **Zvládání bezpečnostních incidentů** obsahuje pravidla a postupy určené pro řešení bezpečnostních incidentů včetně shromažďování potřebných důkazů.
- **Soulad s požadavky** organizace dokladuje naplnění požadavků vyplývajících z právních, smluvních a jiných závazků. [3]

4 ORGANIZAČNÍ ZABEZPEČENÍ INFORMACÍ

Další kategorií, které je věnovaná pozornost a neodmyslitelně je svázána s problematikou bezpečnosti informací, je tzv. **organizační bezpečnost**. Proces zavádění informační bezpečnosti probíhá v několika definovaných etapách, kde má každá z etap definované vstupy, výstupy a nechybí ani terminování zahájení a ukončení jednotlivých etap.

Organizace informační bezpečnosti znázorňuje níže uvedené schéma (Obr. 9). [16]

Obr. 9 Organizační bezpečnost informací. [16]

4.1 Bezpečnostní analýza

Organizační bezpečnost začínáme bezpečnostní analýzou. Jedná se o proces, který podporuje konkrétní situaci důkladnému posuzování stavu, vazeb, příčin, důsledků apod. Pro provádění bezpečnostní analýzy není jednotný model ani přesně stanovená šablona. Stačí si uvědomit, že celý systém informační bezpečnosti stojí a padá na lidech.

Bezpečnostní analýza má vždy velmi podobný průběh:

- identifikace rizik;
- identifikace hrozeb;
- identifikace zranitelných míst;
- návrh opatření. [17]

Na začátku je nutné podrobně stanovit strukturu a hodnotu aktiv, tj. kde jsou skutečně cenná data, jaká je jejich cena i hodnota. Data je zapotřebí podle kritérií rozdělit na několik kategorií. Na základě provedených analýz je nutné stanovit, co hrozí jednotlivým datům. Jakým typům útoků nebo incidentů mohou být vystaveny – vnější vs. vnitřní narušitel, hardwarové selhání, přírodní katastrofy aj. Identifikací zranitelných míst zjišťujeme, s jakou pravděpodobností může dojít k jednotlivým výše zmíněným incidentům a kde jsou slabá místa systému, v nichž by incident mohl vzniknout. Na základě předchozích bodů jsou navrženy organizační i technické prostředky, jejichž cílem je ochránit slabá místa a zamezit nebo alespoň minimalizovat možnost vzniku incidentu. [17]

4.2 Bezpečnostní politika a implementace protiopatření

Bezpečnostní politika představuje „překlopení“ výše získaných informací do praxe. Je to vlastně interní předpis, který vymezuje základní principy bezpečnosti informačního systému. Jedná se o souhrn zásad, pravidel, norem, opatření sloužících k zajištění bezpečnosti. Měla by obsahovat:

- **zásady o datech** v instituci, jak je klasifikovat, jak s nimi nakládat;
- **přidělování oprávnění,** schvalování, rozsah, zodpovědnost, zpětná kontrola, o **kompetencích** pro jednotlivé činnosti;
- **postupy** pro případ závad, nenadálých událostí – hardware, software, přírodní pohromy, s cílem zachování kontinuity provozu instituce.

Bezpečnostní politika se skládá ze dvou typů postupů **periodicky** se opakující a **jednorázové** zavedení bezpečnostních prvků. Jednorázové úkony v rámci bezpečnostní politiky řeší **plán bezpečnosti**. Ten stanoví potřebu nasazení jednotlivých prvků, termíny a priority a to na období:

- **krátkodobé** (administrativní opatření, změny přístupových práv, konfigurace);
- **střednědobé** (školení uživatelů);
- **dlouhodobé** (požadavky při nákupu nového hardware i software).

Součástí je i podrobný popis investic, provozních nákladů i lidských zdrojů. [17]

Bezpečnostní politika by neměla řešit jen běžný provoz, ale i mimořádné situace. Zde můžeme např. zařadit virový útok, zneužití dat apod. Proto je nutné vypracovat **krizový plán**. Většina hrozeb je přesně známá a definovaná.

Krizový plán obsahuje typické scénáře jak:

- reagovat na nejrůznější druhy poruch, havárií a katastrof;
- zajistit kontinuální provoz jednotlivých systémů;
- zajistit fungování celé organizace;
- co nejrychleji odstranit následky incidentu.

Krizový plán by se měl pohybovat nejen v oblasti teoretické, ale popsané postupy by měly být prověřené v praxi. Je vlastně součástí prevence, což je v konečném důsledku vždy levnější než řešení následků vzniklého incidentu a v neposlední řadě brání chaosu. Obsahuje informace o tom jak incident identifikovat, kam ho hlásit, co dělat a role jednotlivých aktérů (uživatel, správce apod.). **Implementace protiopatření** obsahuje studii bezpečnostních opatření a jejich zavedení do praxe. [17]

4.3 Kontrolní audit

Třetím krokem po analýze a bezpečnostní politice je **audit**. Jeho hlavním úkolem je porovnání situace požadované v bezpečnostní politice se skutečnou situací. Auditem zjišťujeme, kde dochází k plnění požadavků stanovených již zmiňovanou bezpečnostní politikou a kde naopak dochází k jejich neplnění a proč. Důvodem neplnění nemusí být pouze nedbalost a nedisciplinovanost, ale také skutečnost, že při navrhování bezpečnostní politiky nebyly vzaty všechny skutečnosti a zavádění některých požadavků do praxe je obtížné nebo přímo nemožné. Bezpečností audit ověřuje stav implementace bezpečnostní politiky a její správné naplňování.

K dalším cílům bezpečnostního auditu patří:

- **poskytnout informace** zda je dosaženo požadovaných kritérií;
- **odhalit nedostatky** v informačním systému nebo bezpečnostní politice;
- **navrhnout možnost nápravy** v případě zjištěných nedostatků. [17]

5 DÍLČÍ ZÁVĚR TEORETICKÉ ČÁSTI

Cílem teoretické části je především vysvětlení základní terminologie a pojmů s touto problematikou související. Hlavní termín, se kterým se setkáváme v celé části práce, je **informace**. Úvodem je objasněna její specifikace a také rozdělení informací z hlediska jejich potřeby ochrany. Součástí úvodní kapitoly je výčet základní legislativy, která se vztahuje k informacím, k jejich bezpečnosti a povinností, které souvisí s jejich ochranou. Zmínka, jen okrajově, je také o organizacích, které se problematikou ochrany a bezpečnosti zabývají.

Více prostoru je v této části věnována **bezpečnosti osobních údajů**. Kapitola objasňuje základní pojmy, se kterými se při práci s osobními údaji setkáváme. Jsou objasněny pojmy, jako je např. osobní údaj, citlivý údaj, ale i kdo to je subjekt údajů, zpracovatel či správce, ale také jak se s těmito údaji dle legislativního vymezení nakládá. Část této kapitoly je věnovaná vývoji zákonných norem ochrany osobních údajů a jejich vzájemné souvislosti.

Kapitola **informační bezpečnost** popisuje systém zajištění bezpečnosti informací v organizaci. Základem kapitoly je vymezení prvků informační bezpečnosti a jejich vzájemné vazby. Celkem přehledně tyto vazby zobrazuje schéma v úvodu této kapitoly. Dále jsou vymezeny úrovně bezpečnosti informací a objasněny vzájemné vazby mezi bezpečností organizace, informační bezpečností a bezpečností IS/IT. Závěrem kapitoly je zmínka o kybernetickém zákoně, jsou vymezeny subjekty, kterých se uvedený zákon týká a objasněna vzájemná vazba informační bezpečnost vs. kybernetická bezpečnost. Posledním tématem této obsáhlejší kapitoly je okrajově zmíněna realizace bezpečnostních opatření, dle příslušné normy. Jednotlivé oblasti těchto opatření jsou shrnuty do jedenácti kapitol a jsou krátce vysvětleny.

Závěrečná kapitola teoretické části je věnována **organizačnímu zabezpečení informací** a popisuje jednotlivé etapy zavádění informační bezpečnosti. Patří zde bezpečnostní analýza, bezpečnostní politika, implementace a kontrolní audit. Etapy jsou popsány a vysvětlen obsah, čím se zabývají.

II. PRAKTICKÁ ČÁST

6 METODIKA PRAKTICKÉ ČÁSTI

Cílem praktické části je definování prostředí zdravotnického zařízení, v němž bude realizována analýza rizik. Úvod je věnován obecnému přehledu, který zahrnuje popis systému zdravotnictví v České republice, včetně legislativního vymezení, kterým se zdravotnictví řídí, až po způsoby nakládání se zdravotnickou dokumentací (ZD).

Pomyslná druhá část této praktické části je věnována **konkrétnímu zdravotnickému zařízení**. Obsahuje krátkou historii a současnost zdravotnického zařízení, Je také znázorněno a pospáno situační schéma a organizační struktura, včetně personálního složení. Po úvodním seznámení se zdravotnickým zařízením se již zaměřuji na samotnou **analýzu rizik** a jejich **vyhodnocení.**

6.1 Použité metody analýzy

Úvodem samotné analýzy v organizaci, je uveden podrobný souhrn stávající situace, který byl proveden vlastním průzkumem. Následuje zpracování analýzy níže uvedenými metodami.

BRAINSTORMING

Brainstorming je skupinová kreativní technika. Cílem je generování co nejvíce nápadů na dané téma. Používá se v celé řadě oblastí a použití je neomezené. Všeobecně je známo pět základních zásad. Jejich cílem je eliminovat veškerá omezení a naopak stimulovat tvorbu nových myšlenek:

- příjemná atmosféra (navodit tvůrčí klima, příjemné prostředí);
- soustředíme se na kvantitu (čím více námětů, tím kvalitní návrh řešení);
- žádná kritika (kritiku odkládáme na později, abychom nebrzdili toky myšlenek);
- jakékoliv nápady jsou vítány (generování námětů bez ohledu na jejich reálnost);
- kombinujeme a zlepšujeme již vzniklé nápady. [18]

WHAT – IF analýza:

Jedná se o jednoduchou analytickou techniku používanou při rozhodování a řízení rizik. Její princip je postaven na hledání možných dopadů vybraných situací. Této analýzy se zpravidla účastní skupina zkušených lidí, která klade otázky nebo vyslovuje možné dopady. Metoda není tak vnitřně strukturovaná jako jiné techniky. Je velmi flexibilní a může se přizpůsobit konkrétnímu účelu. Jejím cílem je identifikace problémů nebo nebezpečných stavů v procesu. Výstupem je popis potenciálních problémů či rizik včetně doporučení, jak jim předcházet (prevence). [18]

SKÓROVACÍ METODA S MAPOU RIZIK

Tato metodou slouží k ohodnocení definovaných rizik. Pro každý rizikový faktor se v této metodě ohodnotí jak možnost výskytu rizikového faktoru, tak její dopad prostřednictvím desetibodové stupnice. Výsledné skóre se vypočte jako aritmetický průměr odhadů jednotlivých hodnotitelů. Na závěr se sestaví mapa rizik jako dvojrozměrná matice ve tvaru bodového grafu. Návrhy na snížení rizika jsou převážně zpracovány pro rizika v kvadrantu kritických rizik a pro kvadrant významných rizik. Samozřejmě mohou být zpracována i pro další rizika, kde je možnost jeho snížení. [19]

6.2 Vyhodnocení a závěr

Závěrem praktické části je shrnutí zjištěných výsledků analýzy rizik a následné doporučení pro jejich snížení včetně doporučení, jak lze definovaná rizika ošetřit a zamezit jejich vzniku. Závěr je věnován shrnutí řešené problematiky a přínosu práce.

7 ZDRAVOTNICKÁ ZAŘÍZENÍ

Hlavním posláním zdravotnických zařízení je **poskytování zdravotní péče,** což je definováno v zákoně č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování. Jedná se o soubor činností, které jsou prováděny za účelem předcházení nemoci, posuzování zdravotního stavu, zmírnění utrpení. Zahrnuje především preventivní, diagnostickou, léčebnou a rehabilitační činnost. Kromě této zdravotní péče poskytují zdravotnická zařízení i jiné zdravotní služby, které zahrnují zdravotnickou záchrannou službu, zdravotnickou dopravní službu, přepravu pacientů aj. [20]

7.1 Soustava zdravotnických zařízení

Soustavu zdravotnických zařízení v České republice tvoří:

- zdravotnická zařízení státu (vojenské nemocnice);
- zdravotnická zařízení obcí a krajů (polikliniky a nemocnice);
- zdravotnická zařízení fyzických a právnických osob (privátní kliniky);
- zařízení pro výchovu, výuku a pro další vzdělávání zdravotnických pracovníků;
- organizace pro zdravotnickou výrobu, pro zásobování léčivy;
- vědeckovýzkumná a vývojová pracoviště na úseku zdravotnictví. [21]

Dle posledních zveřejněných údajů Českého statistického úřadu bylo koncem roku 2013 v ČR evidováno **29 218 zdravotnických zařízení** (Tab. 1) a celkem ve zdravotnictví pracovalo 250 233 pracovníků. Mezi nejpočetnější skupinu patří samostatná ambulantní péče.

Tab. 1 Soustava zdravotnických zařízení v České republice. [22]

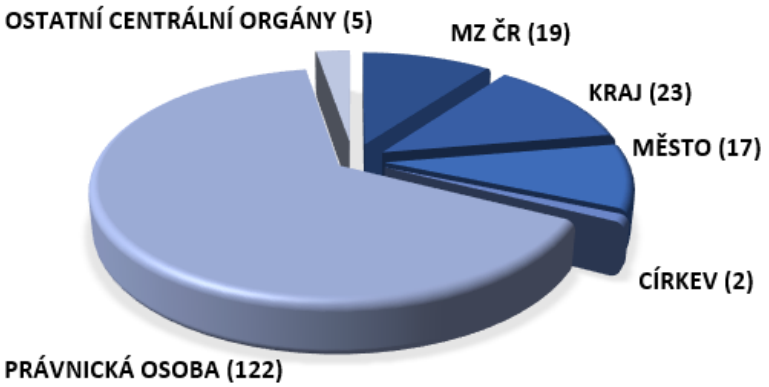
Druh zařízení	Počet zařízení
Nemocnice	**188**
Odborné léčebné ústavy	**158**
Lázeňské léčebny	**81**
Samostatná ambulantní zařízení	**24 979**
Zvláštní zdravotnická zařízení	**368**
Zařízení lékárenské péče	**3 379**
Orgány ochrany veřejného zdraví	**19**
Ostatní	**46**

7.2 Zřizovatelé zdravotnických zařízení

Zřizovatelem zdravotnického zařízení mohou být:

- Ministerstvo zdravotnictví České republiky;
- kraje nebo obce v rámci své samostatné působnosti;
- právnické a fyzické osoby.

V následujícím obrázku (Obr. 10) jsou rozdělena lůžková zdravotnická zařízení ústavní péče (nemocnice) dle zřizovatele. Síť lůžkových zařízení ústavní péče byla v roce 2013 složena ze **188 nemocnic** s celkovým počtem 56 807 lůžek. [22]



Obr. 10 Rozdělení nemocnic dle zřizovatele. [22]

7.3 Druhy zdravotní péče

- Ambulantní péče: jedná se o zdravotní péči, při které není nutná hospitalizace;
- Lůžková péče: pro poskytnutí péče je nezbytná hospitalizace pacienta;
- Zdravotnická záchranná služba: v případě ošetření pacient na místě události;
- Pracovně lékařské služby: hodnotí pracovní způsobilost k práci;
- Dispenzární péče: jedná se o dlouhodobé sledování zdravotního stavu pacienta;
- Lázeňská léčebně rehabilitační péče: je součástí léčebného procesu;
- Poskytování léčivých přípravků a zdravotnických prostředků: lékárenská péče;
- Preventivní péče: primární péče zahrnující preventivní prohlídky, očkování. [23]

8 ZDRAVOTNICKÁ DOKUMENTACE

Veškerá citlivá data pacientů, která se ve zdravotnickém zařízení objevují, jsou součástí **zdravotnické dokumentace**. Co je to vlastně zdravotnická dokumentace?

Žádný právní předpis přesně nedefinuje, co je to vlastně ZD. Pro definování pojmu ZD je tak nutné od sebe odlišit tři pojmy:

- údaj
- záznam údaje
- nosič záznamu

Údajem je myšlena informace. V případě **nosiče záznamu údaje** jde o rukou popsaný, stejně jako potištěný list papíru, pevný disk v počítači a podobně. ZD pak je to, co je na těchto nosičích uloženo a obsahuje příslušné informace. [24]

8.1 Obsah zdravotnické dokumentace

ZD je tedy záznamem, resp. souhrnem všech záznamů, vedených o určitém pacientovi jedním konkrétním zdravotnickým zařízením obsahujícím:

- osobní údaje pacienta potřebné pro identifikaci pacienta a zjištění anamnézy;
- informace o onemocnění pacienta;
- průběh a výsledky vyšetření, způsob léčení.

Tento záznam má podobu písemnou, obrazovou, zvukovou či elektronickou. Vyskytuje s v podobě digitální či analogové. [24]

ZD slouží především pro potřeby **zdravotnických pracovníků**, kterým tyto informace umožňují zvolit správnou léčebnou strategii. Je také zdrojem informací pro samotného **pacienta**. Vedle těchto základních účelů slouží ZD i jako **důkazní prostředek** při sporech, zejména mezi pacientem a zdravotnickým zařízením, nebo také při **řešení různých stížností či připomínek** ke kvalitě poskytnuté péče. Nelze zapomenout, že ZD je také pomůckou při **výuce studentů** lékařství. Je také podkladem pro provádění **auditů kvality** poskytované zdravotní péče. Slouží také jako **důkaz o poskytnuté zdravotní péči**, za kterou zdravotnické zařízení požaduje úhradu od zdravotní pojišťovny. [24]

8.2 Povinnosti správce údajů

ZD je sbírkou převážně citlivých osobních údajů. S tím souvisí povinnost zdravotnických zařízení, jako **správce osobních údajů**, dodržovat požadavky, které ZOOÚ stanoví. Mezi jeho povinnosti uvádí § 5 ZOOÚ tyto:

- stanovit účel, k němuž mají být osobní údaje zpracovány;
- stanovit prostředky a způsob zpracování osobních údajů;
- zpracovat pouze přesné osobní údaje;
- shromažďovat osobní údaje pouze v rozsahu pro naplnění stanoveného účelu;
- uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu zpracování;
- zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny;
- nesdružovat osobní údaje, které byly získány k rozdílným účelům.

Pro vedení ZD zde platí **výjimka,** a to vzhledem k tomu, že zdravotnické zařízení má zákonem uloženou povinnost vést ZD. **Souhlas pacienta tedy nepotřebují**. [24]

8.3 Vlastnictví zdravotnické dokumentace

Zajímavá a sporná je otázka, kdo je vlastníkem ZD.

Zdravotnická zařízení obvykle tvrdí, že jsou vlastníky, protože zakoupila prostředky potřebné k pořízení ZD a nosiče, na kterých je dokumentace vedena. Existuje také jiný názor, že vlastníkem je pacient, neboť o něm je vedena. Třetí názor říká, že vlastníkem je stát. Stát je totiž hlavním garantem péče o zdraví občanů a žádné zdravotnické zařízení nemůže fungovat bez státního souhlasu. Kromě tohoto ZD nelze dědit, darovat, prodat, ani pronajmout. Při zrušení registrace se musí odevzdat. [24]

Vlastník ZD tedy neexistuje, protože ZD není podle českých právních předpisů předmětem vlastnického práva.

V případě zrušení registrace **nestátního zdravotnického zařízení** je provozovatel tohoto zdravotnického zařízení povinen zajistit ZD tak, aby byla chráněna před nahlížením nebo jiným nakládáním neoprávněnými osobami. [24]

Ke zrušení registrace může dojít v případech:

- pozbytí způsobilosti k výkonu zdravotnického povolání;
- závažných porušení hygienických zásad;
- na žádost provozovatele zdravotnického zařízení.

Správní úřad (podle místa provozování zdravotnického zařízení), který vydal rozhodnutí o registraci má povinnost převzít a zajistit ZD tak, aby byla chráněna před nahlížením, neoprávněným nakládáním či ztrátou. Pro návaznost zdravotní péče, mají také povinnost po přechodnou dobu vydávat výpisy, opisy nebo kopie zdravotnické dokumentace. Následně na základně oznámení pacienta, o kterém je dokumentace vedena, ji neprodleně předá zdravotnickému zařízení, které si pacient zvolil.

V případě zrušení registrace **státního zdravotnického zařízení** (v naprosté většině je zřizovatelem MZ ČR) je zřizovatel povinen:

- převzít zdravotnickou dokumentaci;
- zajistit ji před nahlížením, jiným neoprávněným nakládáním nebo ztrátou;
- oznámit tuto skutečnost tak, aby se tom pacienti dozvěděli;
- předávat pacienty nově zvoleným zdravotnickým zařízením;
- v mezidobí vyhotovovat potřebné výpisy, opisy a kopie. [24]

8.4 Nahlížení do zdravotnické dokumentace

Zákon ukládá zdravotníkům jako správcům i specifické povinnosti při jejich ochraně zabezpečení. Zákon výslovně uvádí: *„povinnost přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, a to i po ukončení jejich zpracování“*. V praxi je tak nezbytné mít zdravotnickou dokumentaci v listinné podobě uloženou na bezpečném místě, nejlépe v zámkem opatřené skříni v uzamykatelné místnosti. Pokud se jedná o dokumentaci vedenou elektronicky, tak musí být opatřena přístupovým heslem. [25]

Právo nahlížet do ZD je vymezeno zákonným způsobem a podléhá režimu povinné mlčenlivosti.

Do zdravotnické dokumentace smějí nahlížet, a to **bez souhlasu pacienta**:

- ošetřující lékař, konziliární lékař, rehabilitační pracovník, zdravotní sestra;
- soudní znalci při vypracování znaleckého posudku;
- revizní lékaři zdravotních pojišťoven;
- členové znaleckých komisí;
- nadřízení kontrolující úroveň vedení zdravotnické dokumentace.

Nahlížet dále mohou, ale jen s **písemným souhlasem pacienta**:

- právní zástupce pacienta;
- členové organizace pověřené přešetřením stížnosti pacienta. [24]

8.5 Zásady vyřazování dokumentů

Vyřazováním ZD se rozumí posuzování a výběr ZD, která je nadále pro poskytování zdravotní péče nepotřebná. Při tomto výběru se rozhoduje o tom, zda ZD bude po uplynutí skartační lhůty vyřazena z evidence a navržena ke zničení.

Vyřazování se provádí ve skartačním řízení, které se provádí **jedenkrát za rok** komplexně za celé zdravotnické zařízení. Bez skartačního řízení nelze ZD ničit. Předmětem skartačního řízení je veškerá ZD, u které uplynula skartační lhůta. [26]

S hlediska skartace se písemnosti dělí následovně:

- **Písemnosti A** (archiv): jsou ty, které mají význam z hlediska ekonomického, právního, historického, sociálního a kulturního. Tyto písemnosti se zásadně neskartují, ale archivují se ve Státním ústředním archivu.
- **Písemnosti V** (výběr): jsou písemnosti, které jsou po uplynutí skartační doby odborně posouzeny, vybrané z nich jsou uloženy do Státního ústředního archivu a ostatní jsou skartovány.
- **Písemnosti S** (skartace): jedná se o písemnosti, které se po uplynutí skartační doby skartují (zničí). Skartaci předcházejí skartační řízení. Při skartaci musí být dokumenty fyzicky zničeny, a to s ohledem na ochranu osobních údajů v nich uvedených. [21]

Odborný dohled nad provedením skartace ve zdravotnických zařízeních provádí skartační komise. Členy skartační komise, které jmenuje a odvolává provozovatel zdravotnického zařízení nebo jím určený vedoucí zaměstnanec tohoto zdravotnického zařízení, jsou zdravotničtí pracovníci. [26]

Skartační lhůta:

Tato lhůta určuje dobu, po kterou je nutné uchovat ZD (Tab. 2). Před jejím uplynutím nesmí být ZD zařazena do skartačního řízení. Skartační lhůty jsou stanoveny dle skartačního plánu, který tvoří přílohu č. 3. vyhlášky MZ ČR č. 98/2012 Sb., o zdravotnické dokumentaci. [26]

Tab. 2 Příklady délky archivace. [26]

Druh zdravotní péče	Délka	Poznámka
Ambulantní péče	**5 let**	po posledním vyšetření
Laboratorní výsledky	**5 let**	od provedeného vyšetření
Registrující lékař (gynekolog, praktický lékař)	**10 let**	od změny lékaře, nebo od úmrtí pacienta
Jednodenní péče	**15 let**	od posledního poskytnutí, nebo 10 let od úmrtí pacienta
Záznam o podání transfúzního přípravku	**30 let**	od podání přípravku, nebo 10 let od úmrtí pacienta
Lůžková péče	**40 let**	od poslední hospitalizace, nebo od úmrtí pacienta
Pitevní protokol	**150 let**	ode dne vystavení

Průběh skartačního řízení:

Skartační řízení se zahajuje u ZD, jejíž skartační lhůta uplynula. Pověřený zdravotnický pracovník vypracuje skartační návrh, ke kterému se připojí seznam ZD k vyřazení. Tento návrh se předává skartační komisi, je-li zřízena, k posouzení a souhlasu. Po posouzení komisí je skartační návrh předložen provozovateli zdravotnického zařízení, který po schválení posílá skartační návrh příslušnému archivu provádějícímu u zdravotnického zařízení skartační řízení. [26]

9 ZDRAVOTNICTVÍ A LEGISLATIVA

Každý z nás je pacient a během svého života nutně vstupuje do právních vztahů v souvislosti s medicínou. Poprvé při narození, pak při dětské prevenci, povinném očkování, při péči u svého praktického lékaře, zubního lékaře. Vstoupíme-li do lékařské ordinace, přichází-li lékař k nám, jsme-li hospitalizování, vstupujeme automaticky do právních vztahů s lékaři, dalšími zdravotníky a zdravotnickými zařízeními. [27]

Dnešní doba klade na lékaře a další zdravotnické pracovníky nové požadavky nejen pokud jde o vlastní odbornost. Právní znalosti se u lékařů stávají nezbytnou součástí jejich specializační průpravy. Lékař musí znát správnou odpověď na řadu mnohdy nikoli jednoduchých otázek. O čem a v jakém rozsahu pacienta informovat? Koho z pacientových blízkých informovat a v jakém rozsahu? Má pacient a jeho blízcí právo na přístup do zdravotnické dokumentace? Má lékař zachovat povinnou mlčenlivost i vůči policii? Kdy je vázán povinnou mlčenlivostí, a kdy naopak má oznamovací povinnost? Takto by bylo možno sepsat desítky dalších velmi aktuálních otázek, na které lékaři při své každodenní praxi hledají správou odpověď. Před patnácti lety bylo porušení povinné mlčenlivosti etickým proviněním, nyní je trestným činem s trestní sazbou jeden až pět let odnětí svobody. [27]

9.1 Zabezpečení citlivých dat

- **101/2000 Sb., o ochraně osobních údajů.**

Základní legislativa zaměřená na zabezpečení citlivých dat je **zákon č. 101/2000 Sb., o ochraně osobních údajů**. Již samotný zákon o zdravotních službách upozorňuje na vícero místech, že vedení ZD je vlastně zacházení s osobními údaji a že práva a povinnosti při zpracování s osobních údajů v souvislosti s poskytováním zdravotní péče se řídí tímto zákonem. Zdravotnická zařízení mají povinnost dodržovat požadavky stanovené zákonem. [24]

Problematika ochrany osobních údajů, včetně vymezení základní terminologie je podrobně rozepsána již v kapitole druhé v teoretické části.

9.2 Zdravotnická dokumentace

- **372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování;**
- **Vyhláška č. 98/2012 Sb., o zdravotnické dokumentaci;**
- **89/2012 Sb., občanský zákoník;**
- **373/2011 Sb., o specifických zdravotnických službách.**

Základním **zdrojem informací**, které podléhají povinné mlčenlivosti a ochrany osobních údajů, je ve zdravotnickém zařízení již několikrát zmiňovaná **zdravotnická dokumentace**.

Historicky nejstarší zmínka o ZD v právním předpisu na úrovni zákona se objevila v zákoně č. 160/1992 Sb., o zdravotní péči v nestátních zdravotnických zařízení. Od té doby se uvádí též povinnost vést ZD.

V základním právním předpise regulujícím poskytování zdravotní péče v České republice, v zákoně č. 20/1966 Sb., o péči a zdraví lidu (ZPZL), se otázka ZD začala řešit až mnohem později.

Je s podivem, že tento zákon nebyl až do roku 1990 ani jednou novelizován a v nezměněné podobě „přežil“ bezmála čtvrt století. V porevolučním období byl naopak mnohokrát novelizován a až v roce 2011 zcela nahrazen **zákonem č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování** (ZZS). [24]

Posledním novým právním předpisem z oblasti dokumentace je **vyhláška č. 98/2012 Sb., o zdravotnické dokumentaci** (její poslední novelizace byla provedena vyhláškou č. 362/2015 Sb., s účinností od 1. 1. 2016). Tato vyhláška je členěna do osmi paragrafů a stejně jako předchozí vyhlášky má také tři přílohy, které specifikují jednotlivé druhy dokumentace a nakládání s nimi. [28]

9.3 Mlčenlivost

- **372/2011 Sb., o zdravotnických službách a podmínkách jejich poskytování.**

Povinná mlčenlivost v resortu zdravotnictví je ošetřena v zákoně číslo **372/2011 Sb., o zdravotnických službách v § 51**, který pojednává o zachování mlčenlivosti o všech skutečnostech, o kterých se poskytovatel zdravotních služeb dozvěděl v souvislosti s poskytováním zdravotních služeb. [29]

Poskytování zdravotní péče sebou denně v oblasti povinné mlčenlivosti přináší nejrůznější varianty problémů – příbuzní si stěžují na nedostatek informací o zdravotním stavu osob blízkých, na to, že zdravotníci informují jen některé příbuzné či na skutečnost, že jim zdravotníci brání v nahlížení do zdravotnické dokumentace, ať již žijícího nebo zemřelého člena rodiny. Ze strany zdravotnického pracovníka je také nutné brát v potaz důvod, proč příbuzní chtějí nahlédnout do ZD, např. zda chtějí přezkoumat zdravotní péči nebo zda jejich příbuzný netrpí či netrpěl dědičnou chorobou. I v těchto situacích je proto nutné brát v úvahu citlivost mezilidských vztahů vznikajících v rámci zdravotní péče, na něž právní úprava nedokáže vždy úspěšně reagovat a nabídnout jednoznačný návod na jejich řešení. [29]

Subjektem, na který povinnosti vyplývající z mlčenlivosti dopadají nejvíce, je přirozeně zdravotnický pracovník. Povinnou mlčenlivostí je tedy vázán **každý zdravotnický pracovník,** tedy nikoliv jen lékař, ale i další zdravotničtí pracovníci vykonávající zdravotnické povolání ve smyslu příslušných právních předpisů. Mlčenlivosti jsou konečně vázáni i ostatní zaměstnanci zdravotnických zařízení, a to i ti, kteří zdravotnické povolání nevykonávají. [29]

Povinnost mlčenlivosti však není absolutní a může být prolomena. A to legislativním nařízením nadřízeným orgánem v důležitém stáním zájmu, v případě ohlašování povinností stanovené zvláštním právním předpisem (např. národní zdravotní registry) a také se souhlasem dotčené osoby (pacienta). [21]

V případě **souhlasu** pacienta s poskytováním informací týkající se jeho zdravotního stavu, musí mít vždy **písemnou formu**. Hlavní součástí souhlasu je označení osoby, které mohou být na základě souhlasu informace sděleny. Doba udělení souhlasu se neuvádí, ale může být kdykoliv odvolán. Zákon také dává pacientovi i opačné právo, tj. právo vyslovit zákaz s podáváním informací o zdravotním stavu. Souhlas musí být vždy součástí ZD a opatřen **podpisem** ošetřujícího lékaře a pacienta. Každé nahlédnutí do ZD se zaznamenává. [29]

10 ZDRAVOTNICKÁ INFORMATIKA

Velmi častým zásahem do práva na ochranu osobních údajů je i volné zpřístupnění údajů o pacientech v rámci **nemocničního informačního systému** (NIS). I pro případ vedení těchto informací v elektronické podobě, která připouští sdílení, zákon o ochraně osobních údajů stanoví poskytovatelům zdravotních služeb několik důležitých povinností.

Především je to povinnost zajistit, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze oprávněné osoby, aby i tyto osoby měly přístup pouze k údajům, které se týkají jimi zabezpečované oblasti zdravotních služeb, a aby byla vedená přesná evidence o tom, který zdravotník či administrativní pracovník zdravotnického zařízení se na jaké informace o pacientovi kdy díval a z jakého důvodu. [25]

10.1 Přehled zdravotnických informačních systémů

- samostatných ordinací praktických a odborných lékařů;
- nemocniční informační systémy včetně ambulancí a poliklinik;
- pro sběr a zpracování statistických dat (ÚZIS);
- jednotlivých zdravotních registrů (ÚZIS, KSRZIS);
- zdravotních pojišťoven (VZP);
- hygienické služby (KHS, SZÚ, KSRZIS);
- pro řízení zdravotnictví (MZ ČR a KÚ);
- knihoven a vědecké informatiky včetně expertních systémů (IPVZ, NLK). [30]

10.2 Informační systém zdravotnického zařízení

Informační systém zdravotnického zařízení pořizuje, zpracovává a archivuje údaje o:

- rozsahu, průběhu a efektivitě poskytované léčebné péče;
- zdravotním stavu jednotlivých ošetřovaných osob;
- ekonomice zařízení;
- materiálním zajištění provozu;
- organizaci práce a personálním obsazení;
- správě zdravotnického zařízení, a ostatních aktivitách zdravotnického zařízení. [30]

10.3 Klíčová legislativa

- Zákon č. 101/2000 Sb., o ochraně osobních údajů (správce, zpracovatel, archivace, zpracovávání dat, anonymizovaná data pro vědu);
- Zákon č. 227/2000 Sb., o elektronickém podpisu (zaručený elektronický podpis pro zdravotnickou dokumentaci, certifikační autorita pro zdravotnictví, časové razítko);
- Zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zmocnění k existenci národních zdravotních registrů);
- Zákon č. 258/2000 Sb., o ochraně veřejného zdraví (zmocnění k existenci registrů hygienické služby);
- Zákon č. 285/2002 Sb., o darování, odběrech a transplantacích tkání a orgánů.
- Vyhláška 385/2006 Sb., o zdravotnické dokumentaci;
- Vyhláška 301/2006 Sb., o způsobu předepisování léčivých přípravků. [30]

10.4 Nemocniční informační systém

Nemocniční informační systémy – označovány jako NIS, se dělí na jednotlivé moduly:

- **Příjem:** centrální registr pacientů.
- **Ambulance**:
    - systém vedení ambulance;
    - termínovaný plán;
    - evidence výkonů.
- **Lůžková oddělení**:
    - objednávání pacientů;
    - organizace služeb;
    - evidence pacientů, lůžek, medikace;
    - zdravotnická dokumentace, příjem, propouštěcí zprávy;
    - výsledkové listy, kumulativní nálezy, konzultace;
    - výstup do zdravotního pojištění;
    - výstup do registrů a statistiky. [30]

11 ZDRAVOTNICKÉ ZAŘÍZENÍ ABC

Pro zpracování praktické části této bakalářské práce jsem si vybrala zdravotnické zařízení, které se nachází v místě mého bydliště a jsem zde současně i zaměstnancem. Čerpání informací z vybraného zdravotnického zařízení a realizovaný průzkum potřebný pro zpracování analýzy rizik, jsem prováděla s písemným se souhlasem vedení nemocnice s omezením, že zdravotnické zařízení budu uvádět pod smyšleným názvem.

11.1 Historie

Počátky stále zdravotnické péče v tomto městě nacházíme v letech 1802 – 1804. V této době byly zřizovány při výskytu epidemií, většinou moru či cholery, nemocnice nouzové, které ve chvíli, kdy byla epidemie zažehnána, byly zlikvidovány. První oficiální nemocnice ve městě byla vybudována díky dobrovolným sbírkám v červenci 1804, kdy byl přijat první pacient. Do konce roku bylo hospitalizováno 17 pacientů. Začínající nemocnice měla v době svého začátku šest lůžek. Tato nemocnice existovala až do roku 1855. Kapacita samozřejmě pro potřeby města byla nedostačující. Zatímco v roce 1804 bylo hospitalizováno 17 pacientů, od roku 1842 se zde léčilo ročně více než stovka obyvatel.

Přes další sbírky a snahy trvalo osmdesát let, než byl vystavěn na jiném místě zcela nový objekt. Samotná budova byla dílem místního stavitele a byla hotova na podzim roku 1884. Nová nemocnice nesoucí jméno korunního prince Rudolfa, byla slavnostně předána veřejnosti 4. října 1884, tedy téměř před 132 lety. To byl ovšem začátek vývoje, trvajících dalších sto a více let, než se nemocnice rozrostla do dnešního moderního komplexu. [31]

11.2 Současnost

Zdravotnické zařízení, tak jak ho známe v dnešní podobě, poskytuje **komplexní zdravotní péči a patří mezi 106 špičkových zdravotnických zařízení v Česku**, kterým se podařilo získat certifikát Společné akreditační komise. Původně krajská nemocnice s poliklinikou se před pár lety změnila na soukromou společnost, jejíž zřizovatelem je právnická osoba. Díky této změně prošla nemalou rekonstrukcí, modernizací a souvisejícími organizačními změnami. Do její spádové oblasti patří více jak 170 000 obyvatel. Aktuálně disponuje téměř 400 lůžky akutní a následné péče a ročně je zde průměrně hospitalizováno 24 500 pacientů. Ve statistických číslech zdravotnického zařízení je průměrná roční obsazenost lůžek z celkové kapacity nemocnice 80%.

11.3 Orientační plán

Obr. 11 Orientační schéma zdravotnického zařízení. (vlastní zdroj)

Celý komplex zdravotnického zařízení (Obr. 11) se skládá z **hlavní budovy** (s označením 1, 3, 4, 4a), která je hned naproti hlavního vstupu do areálu nemocnice a je určena pro pacienty. V tomto největším objektu jsou umístěny ambulance společně s lůžkovými odděleními a operačními sály (chirurgie, traumatologie, ortopedie, gynekologie, porodnice, ARO, MOJIP, ORL, urologie), speciální ambulance (nutriční, obezitologie, kožní) a také vyšetřovny zobrazovacích metod, jako je RTG. CT a ultrazvuk.

Dalším objektem, určený také zejména pro pacienty je **pavilon interních oborů** (s označením 5, 5a). Zahrnuje také ambulance s možností hospitalizace pacientů (interní, plicní, onkologické a neurologické oddělení) a další poradny (kardiologická, revmatologická, klinické psychologie a logopedie).

Třetím objektem, kde se nacházejí hospitalizovaní pacienti včetně možnosti ambulantního vyšetření je **dětské oddělení** (budova označena č. 6). Budova je určena především pro dět-

ské pacienty. Je zde, mimo lůžkového oddělení, také dětská pohotovostní služka a speciální ambulance dětské kardiologie a alergologie.

Další budovy, kde se ještě můžeme setkat s pacienty, jsou budovy:

transfúzního oddělení (budova č. 7), která slouží dobrovolným dárcům krve a krevní plazmy, **oddělení radioterapie** (budova č. 26), kde se ambulantně léčí onkologicky nemocní pacienti a budova **zobrazovacích metod** (budova č. 16). V této budově se nachází oddělení zobrazovacích metod a to MRI a CT. Pacienti jsou zde opět jen ambulantně vyšetřeni.

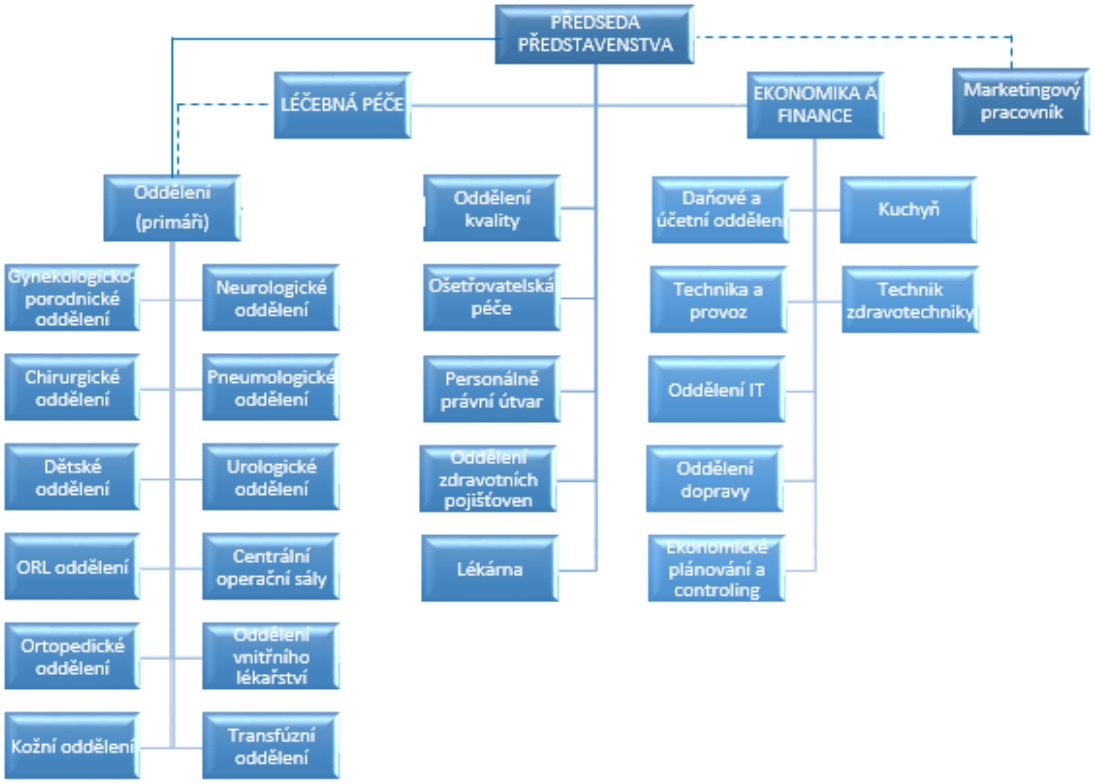
Speciální zdravotní budova je oddělení **patologie a laboratoř.** Zde se mimo jiné provádí laboratorní vyšetření krve, odebraných biologických materiálů (tzv. histologické vyšetření), pitvy zemřelých. Zde se setkáme pouze s lékaři a zdravotnickým personálem.

Budova **Podatelny** (budova č. 8) je určena převážně administrativě. Včetně samotné podatelny, kde se shromažďuje a eviduje veškerá příchozí a odchozí pošta, je zde umístěn i hlavní archiv zdravotnické dokumentace a kancelář referenta spisové a skartační služby. Dále v této budově je kancelář správce budov, technika zdravotnické techniky, oddělení zdravotní pojišťovny a nově je zde přestěhováno oddělení OIT.

Ve schématu není zobrazena budova, kde je se nachází **vedení nemocnice**, ekonomické oddělení, mzdové oddělení, personální oddělení. Tato budova stojí samostatně, tzn. mimo zobrazený areál, a je umístěna vedle hlavní brány nemocnice. Opět se jedná o administrativní budovu, kde se z větší části pohybují THP pracovníci. Pouze přízemní část budovy, kde je umístěna pokladna, se s můžeme potkat s pacienty.

11.4 Organizační struktura

Schéma organizační struktury je standardně rozděleno na jednotlivé úrovně řízení, kterým je svěřeno vedení části organizace (Obr. 12).



Obr. 12 Organizační struktura zdravotnického zařízení. (vlastní zdroj)

11.5 Personální složení

Údaje o personálním složení zdravotnického zařízení jsou aktualizovány každý rok. V současné době (stav k 31. 3. 2016) má nemocnice celkem 947 zaměstnanců. Oproti předchozím rokům došlo k nárůstu počtu zaměstnanců a to především na pozicích ošetřovatele, zdravotnického asistenta a v menší míře i na pozici lékaře. Naopak ke snížení došlo na pracovní pozici všeobecné zdravotní sestry.

V následujícím přehledu (Tab. 3) je uveden seznam pracovních pozic včetně počtu zaměstnanců i dle pohlaví (Obr. 13), kteří ve zdravotnickém zařízení pracují. Zaměstnanci ve zdravotnické zařízení, tak jako i v jiných organizacích, jsou rozděleni dle jejich odborné způsobilosti a získané specializace. Takto jsou hlavně rozděleny pozice lékařů a zdravotnického personálu (ZP).

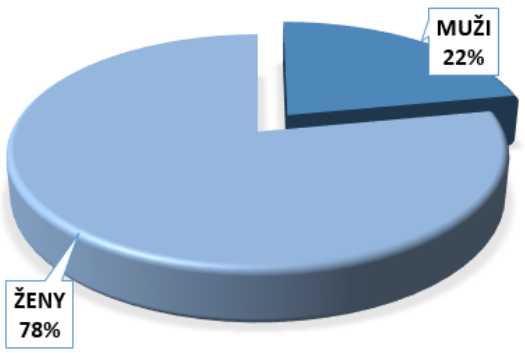
Tab. 3 Celkový počet zaměstnanců. (vlastní zpracování)

Kategorie pracovníků	Počet	Z toho ženy
Lékaři	177	78
Farmaceuti	4	4
Sestry a porodní asistentky	384	374
ZP odborná způsobilost, ostatní odborní pracovníci	53	45
ZP specializovaná způsobilost	16	16
ZP odborný dohled	215	156
THP, dělničtí a provozní pracovníci	98	65
CELKEM	**947**	**738**

U lékařů jsou kategorie rozděleny dle získané specializace na lékaře s odbornou způsobilostí, s odbornou způsobilostí bez odborného dohledu a specializovanou způsobilostí nebo zvláštní odbornou způsobilostí.

Do kategorie ZP s odbornou či specializovanou způsobilostí jsou zařazeny například: radiologický asistent, zdravotnický laborant, nutriční terapeut, zdravotnický záchranář, fyzioterapeut, asistent ochrany veřejného zdraví aj. Tuto kategorii lze definovat tím, že se jedná o zdravotnický personál, který pracuje zcela samostatně na pracovištích dle získané odbornosti. Na druhé straně je kategorie ZP vyžadující odborný dohled. V praxi to znamená, že nad těmito zaměstnanci při vykonávaní jejich pracovních činností musí dohlížet ZP se získanou odbornou popřípadě specializovanou způsobilostí. Patří zde například: zdravotnický asistent, ošetřovatel, sanitář, řidič dopravy nemocných a raněných, masér aj.

Ostatní kategorie pracovníků (THP, dělničtí a provozní pracovníci) zahrnují standardní administrativní zaměstnance, pracovníky údržby apod.



Obr. 13 Poměr zaměstnanců dle pohlaví. (vlastní zdroj)

12 ANALÝZA SOUČASNÝCH RIZIK V ORGANIZACI ABC

Analýza současných rizik začíná vlastním průzkumem stávajícího nastavení bezpečnostních opatření v organizaci a následných rozhovorů se zaměstnanci.

12.1 Popis stávající situace ve zdravotnickém zařízení

Zabezpečení zdravotnického zařízení, jako celku, nelze, jako například standardní firmu s přesně daným provozem, striktně zajistit. Vstup do areálu nemocnice je realizována dvěma vstupy. Jedná se o hlavní vstup, který je zajištěn závorou a vrátnicí, kterou vjíždí během dne (ale i v noci) osobní vozidla zaměstnanců, pacientů, sanitní a vozy záchranné služby, ale i zásobování a vozidla zajišťující technickou údržbu areálu. Druhá vstupní brána je umístěna s tzv. zadní strany nemocnice a je určena pouze pro průchod osob.

Pravidla pro vjezd do areálu je dán vnitřní směrnicí, která má jistá omezující pravidla pro vjezd do areálu zdravotnického zařízení. Co se týká vstupu na jednotlivé pracoviště a oddělení, je vstup samozřejmě pro pacientky a návštěvníky omezen vnitřním řádem nemocnice.

Na jednotlivé pracoviště je přístup pro zaměstnance řešen v rámci klíčového režimu. Směrnice, která řeší nastavení klíčového režimu, přesně definuje, jaké jsou povinnosti vedoucích zaměstnanců týkající se klíčového režimu. Dle této směrnice mají být klíče uschovány na jednotlivých odděleních vždy u vrchní sestry nebo vedoucího pracovníka. Vrchní sestra proti podpisu do osobní karty zaměstnance předává klíče od jednotlivých místností. Náhradní klíče od oddělení se ukládají na vrátnici. Tyto klíče slouží pouze pro případ havárie! Výdej těchto klíčů se provádí záznamem do knihy zápůjček (uvádí se datum předání, osoba, která klíče převzala, datum vrácení a podpis pracovníka vrátnice).

Na jednotlivých pracovištích je nastaven individuální klíčový režim a způsob uschování a předávání klíčů. Ve výstupní analýze bude zahrnuta i tato problematika.

Vydaná bezpečnostní pravidla:

- Havarijní řád;
- Systém vjezdu a parkování v areálu nemocnice;
- Organizace zabečení budov a havarijní klíčový režim.

Zdravotnická dokumentace v praxi

Příjem na oddělení respektive první kontakt pacienta se zdravotnickým personálem standardně probíhá přes příjmovou ambulanci (Obr. 14). Při vstupu do ambulance je pacient vyzván zdravotní sestrou k předložení **průkazu zdravotní pojišťovny** a **předložení občanského průkazu**. Na základě těchto dokladů je zdravotním pracovníkem ověřena totožnost a zaznamenány údaje nezbytné k zaevidování pacienta do kartotéky daného oddělení a k založení ZD. Pacient je dotazován na osobní, zdravotní a další potřebné údaje, které poskytovatel zdravotních služeb potřebuje k zajištění péče.

Obr. 14 Recepce ambulance. (vlastní zdroj)

Před přijetím je pacient lékařem seznámen se všemi potřebnými informacemi a o léčebném plánu. Pacient má samozřejmě právo znát jména ošetřujícího lékaře, sester a dalších pracovníků nemocnice, se kterými bude v kontaktu. Zaměstnanci mají vizitku se svým jménem a pracovní pozicí, kterou v nemocnici zastávají.

Při příjmu k hospitalizaci je pacientovi přiděleno lůžko (pro evidenci zdravotnických pracovníků má číselné označení, které obsahuje číslo pokoje a číslo lůžka, např. 2/3). Oblečení a osobní věci jsou uloženy ve skříni na pokoji a jsou sestrou zaevidovány. **Evidenční lístek**, se seznamem uložených věci je vložen do ZD. Pokud má u sebe pacient nějaké cen-

nosti, či větší částku peněz, je možno tyto věci uložit do úschovny v nemocnici. Pacient samozřejmě dostává doklad o převzetí a uložení.

Součástí příjmu k hospitalizaci je i podpis písemného **Souhlasu s hospitalizací.** Součástí tohoto souhlasu je i možnost odmítnutí přítomnosti osob, které nejsou na poskytování zdravotních služeb přímo zúčastněny a také osob, které se připravují na výkon svého zdravotnického povolání. Je nutné také lékaři sdělit, komu z blízkých osob lze poskytovat informace ohledně zdravotního stavu. Pro telefonické podávání informací se vyžaduje uvedení hesla, které musí volající osoba použít, aby mohly být poskytnuty informace. Heslo i určené osoby se zaznamenávají ve vstupním písemném formuláři s názvem **Záznam o souhlasu s poskytováním informací**.

V souvislosti s některými výkony (způsob léčby, operační výkon, podání anestezie, aj.) je podepisován další dokument, tzv. **Informovaný souhlas**. Jedná se o souhlas s tím, že byl pacient náležitě seznámen a podstupuje vyšetření či výkon dobrovolně.

Pacient může samozřejmě svůj názor změnit a zákrok odmítnout. Po seznámení s důsledky odmítnutí péče, je nutné podepsat odvolání souhlasu, tzv. **Negativní revers** a to za přítomnosti svědka.

Obr. 15 Kartotéka ambulantních karet pacientů. (vlastní zdroj)

Údaje o pacientovi a jeho zdravotním stavu je obsažena v **ambulantní kartě** pacienta, **chorobopisu** a v **elektronickém nemocničním informačním systému**. Součástí ambulantní karty je většinou žádanka o vyšetření od odesílajícího lékaře, výsledky ambulantních vyšetření a zpráva z vyšetření, tzv. ambulantní zpráva. Nezbytným dokumentem je souhlas pacientka s vyšetřením. Tato ambulantní karta je standardně umístěna v **kartotéce na recepci** dané ambulance (Obr. 15). Zde je přístup pouze pro zdravotnický personál daného oddělení.

Chorobopis pacienta, při hospitalizaci, je umístěn na lůžkovém oddělení v **sesterně** s přístupem pouze pro zdravotnický personál daného oddělení (Obr. 16). Tato dokumentace je uložena ve složkách s označením příslušného pokoje a lůžka (například 3/1) a obsahuje všechny potřebné souhlasy, kompletní lékařskou a sesterskou dokumentaci, zprávy, výsledky vyšetření, operační protokol a další dokumenty nezbytné k léčbě pacienta.

Obr. 16 Pracovna sester na lůžkovém oddělení. (vlastní zdroj)

K **elektronické zdravotnické dokumentaci**, která ve větší míře duplikuje papírový chorobopis a poskytuje tiskový výstup, mají přístup zdravotničtí pracovníci přes **přihlašovací údaje**. Práva k přístupu do informačního systému přiděluje oddělení informačních techno-

logií na základě **žádosti vedoucího** zaměstnance (např. primář, staniční sestra). Evidenci přidělených přístupů je v kompetenci oddělení informačních technologií nemocnice.

Chorobopis pacienta je po celou dobu hospitalizace umístěn na oddělení. Při ukončení této hospitalizace je staniční sestrou zkompletován a předán dokumentační pracovnici daného oddělení k vyúčtování poskytnuté péče. Ta po zaúčtování všech provedených výkonů a poskytnutých léků předává chorobopis k další kontrole, a to na **oddělení zdravotnických pojišťoven**. Předem určený pracovník, dle přiděleného oddělení, provádí závěrečnou kontrolu správnosti vykázané péče. Následně je chorobopis vrácen zpět na oddělení dokumentační pracovnici, která vede archiv zdravotnické dokumentace daného oddělení. Dokumentace v příruční registratuře (Obr. 17) zůstává zpravidla 1 – 3 roky od jejich vzniku. Tato registratura slouží k ukládání živé agendy potřebné pro běžnou provozní činnost oddělení. Dokumentační pracovnice po dobu než předá dokumentaci do centrálního archivu, na chorobopisy ručí.

Obr. 17 Příruční archiv dokumentační pracovnice. (vlastní zdroj)

Po uplynutí stanovené doby (většinou po domluvě s hlavní archivářkou) jsou chorobopisy předávány do **centrálního archivu** nemocnice. Předávání probíhá na základě **předávacího protokolu** vypracovaného dokumentační pracovnicí, který obsahuje:

- předávající oddělení;
- jméno a příjmení předávajícího;
- pořadové číslo dokumentu;
- druh (název) dokumentu;
- jmenný seznam pacientů včetně rodných čísel a data ukončení hospitalizace,
- rok vzniku;
- skartační znak.

Při předání je předávací protokol opatřen datem předání, podpisem a razítkem předávajícího a přijímacího pracovníka. Dokumentace je zpravidla uložena v archivačních složkách, o šířce cca 10 cm. Tyto složky jsou opatřeny čelními štítky, na kterých jsou uvedeny požadované údaje.

V **centrálním archivu** dokumentace zůstává po celou dobu až do realizace skartačního řízení.

Do ZD, která je již uložena v centrálním archivu, je možno **nahlížet** pouze na **základě písemné žádosti**, která byla adresována na sekretariát společnosti. Zaměstnanci mohou vstupovat do prostor spisovny (archivu) pouze za doprovodu referenta spisové a skartační služby. Mohou nahlížet pouze do dokumentů svého oddělení. Nahlížení do dokumentů v archivu se eviduje v **Knize návštěv**. Zdravotnická dokumentace se ze spisovny **nesmí vynášet**. Za nahlížení do dokumentace odpovídá referent spisové a skartační služby.

Při ztrátě, nebo poškození dokumentace, se **vyhotovuje zápis** obsahující příčiny, míru zavinění, eventuálně následky ztráty nebo zničení a určit způsob nahrazení dokumentu nebo jiná opatření. Zápis podepisuje vedoucí oddělení, jehož dokument byl poškozen, zničen nebo ztracen. Pokud by existovalo důvodné podezření, že ztrátou, zničením, poškozením nebo zneužitím byl spáchán trestný čin, předkládá se zápis řediteli, který rozhodne o dalším postupu.

Dokumenty jsou ve spisovně uloženy po dobu **stanovenou skartační lhůtou**, uvedenou ve **skartačním plánu**. U ZD (chorobopisu) začíná běžet skartační lhůta posledním rokem hospitalizace. Skartační lhůty nelze zkracovat. Skartační řízení se provádí jednou ročně

kompletně za celé zdravotnické zařízení. Pro řádné provedení skartačního řízení je nezbytná řádná před archivační péče o dokumenty, tj. přesná evidence, správné označení skartačními znaky a lhůtami, přehledné uložení v příručních registraturách a v samotné spisovně (hlavním archivu).

Při **skartačním řízení** vypisuje referent spisové a archivační služby z předávacích protokolů dokumentů „S“ položky, kterým v kalendářním roce uplynula skartační lhůta. Tento seznam, který je doplněný kopiemi předávacích protokolů dokumentů „A“, předaných v uplynulém kalendářním roce do archivu společnosti a žádostí o schválení skartace, podepsanou ředitelem, tvoří **skartační návrh**. Tento návrh zasílá referent spisové služby Zemskému archivu v Opavě (seznamy zasílá vždy dvojmo). Jakmile je Zemským archivem vysloven **souhlas ke skartaci**, lze navržené položky **fyzicky vyřadit**. Za celý proces skartačního řízení odpovídá referent spisové služby.

Vydaná bezpečnostní pravidla v organizaci (směrnice):

- Zdravotnická dokumentace;
- Příjem, překlad a propuštění pacienta a vedení zdravotnické dokumentace;
- Skartační řád;
- Poskytování informací ze zdravotnické dokumentace;
- Provozní řád OIT oddělení;
- Havarijní řád;
- Organizace zabezpečení budov a havarijní klíčový režim.

12.2 Analýza rizik

V průběhu měsíce dubna 2016 byl proveden průzkum v organizaci s cílem zjištění a vyhodnocení rizik, které souvisí s ochranou citlivých údajů pacientů.

Pro analýzu byla zvolena jednoduchá analytická metoda **What – If** (Co se stane když?) s cílem hledání možných dopadů vybraných situací.

Pro vyhodnocení rizik jsem v organizaci oslovila zaměstnance, kteří se s problematikou ochrany dat ve zdravotnickém zařízení, především s práci se ZD denně setkávají. Jednalo se o tyto pozice:

- garant pro lékařské obory;
- manažer kvality;
- referent spisové a skartační služby;
- staniční sestra oddělení;
- dokumentační pracovnice;

Hodnocení rizik probíhalo formou **brainstormingu** a následných **rozhovorů** s náhodně vybranými zaměstnanci organizace.

Po provedeném brainstormingu, rozhovorech se zaměstnanci, ale i z vlastních pracovních zkušeností v této organizaci, vyšla najevo níže uvedená rizika (Tab. 4), která jsou okomentována a ohodnocena **skórovací metodou** (Tab. 5 – 9). Závěrem analýzy je znázorněna **mapa rizik** (Obr. 18), která rozděluje jednotlivá rizika do 4 kvadrantů dle pravděpodobnosti výskytu a dopadu na organizaci.

12.3 Definovaná rizika

Tab. 4 Definovaná rizika. (vlastní zpracování)

Pořadové číslo rizika	Definované riziko
1.	Ztráta dokumentace
2.	Únik citlivých informací
3.	Ztráta klíčů
4.	Neoprávněný přístup k informacím
5.	Neznalost a nedodržování legislativy

12.4 Ohodnocení rizik

Riziko č. 1: Ztráta dokumentace

ZD pacienta je hlavní zdroj citlivých údajů pacienta. Ke ztrátě této dokumentace může dojít během hospitalizace, kdy může dojít díky nedbalosti zdravotnického pracovníka k odcizení či zničení. K další ztrátě může dojít také při následné manipulaci s touto dokumentací po propuštění pacienta. A to vzhledem k tomu, že s dokumentací se dále pracuje. Než se dokumentace archivuje v hlavním archivu, ze kterého se již dokumentace standardně nevydává, zůstává na příslušném oddělení v příručních registraturách. Z těchto registratur se průběžně předává na kontrolu vykázaných výkonů na oddělení zdravotních pojišťoven, ke kontrolnímu auditu, ale také v případě další návštěvy pacienta se zapůjčuje na ambulanci k nahlédnutí lékaři. Přesný pohyb dokumentace není evidován. Během celého procesu s dokumentací může dojít ke ztrátě, popřípadě zničení zdravotnické dokumentace.

Ke ztrátě může dojít také bez zavinění zaměstnance a to v případě živelné pohromy, jako je například požár, povodeň nebo vloupáním ve zdravotnickém zařízení.

Důsledek: ztráta věrohodnosti zdravotnického zařízení, porušení ZOOÚ.

Tab. 5 Ztráta dokumentace. (vlastní zpracování)

Kvantifikace rizik	1.	2.	3.	4.	5.	Skóre (Ø hodnoty)	
Možnost výskytu (1 min. – 10 max.)	5	6	7	8	4	**6**	x
Dopad (1 min. – 10 max.)	9	9	9	9	9	**9**	x
Ocenění rizika = skóre pravděpodobnosti x skóre dopadu							**54**

Rizikový faktor č. 2: únik citlivých informací

K úniku citlivých informací může dojít při porušení povinné mlčenlivosti zaměstnanců. K úniku může dojít při podávání informací o zdravotním stavu (telefonicky, osobně) neoprávněné osobě, kdy si zdravotnický pracovník neověří, komu může informace podávat. Seznam osob, kterým se smí podávat informace, uvádí pacient již při vstupním vyšetření na ambulanci. K úniku informací může také dojít při nedodržení vnitřních předpisů, tj. opomenutí uložení dokumentace do zabezpečené oblasti (kartotéky), nezabezpečení určenými prostředky (uzamknutí místnosti, neodhlášení z počítače), nedbalostí při skartaci aj.

Důsledek: porušení ZOOÚ, výpověď z PP, finanční postih zaměstnanci.

Tab. 6 Únik citlivých informací. (vlastní zpracování)

Kvantifikace rizik	**1.**	**2.**	**3.**	**4.**	**5.**	**Skóre (Ø hodnoty)**	
Možnost výskytu (1 min. – 10 max.)	3	3	4	3	6	**3,8**	x
Dopad (1 min. – 10 max.)	5	8	5	4	6	**5,6**	x
Ocenění rizika = skóre pravděpodobnosti x skóre dopadu							**21**

Rizikový faktor č. 3: ztráta klíčů

Riziko ztráty klíčů vzniká v případě nedbalostního jednání zaměstnance nebo při krádeži. Při ztrátě může následně dojít k neoprávněnému vniknutí do prostor, kde je umístěna nejen zdravotnická dokumentace, ale i léky, elektronická a zdravotnická technika. Riziko stoupá v případě nenahlášení této ztráty a okamžité nezajištění výměny všech zámků od dveří, do kterých měl daný zaměstnanec přístup, tj. nedodržením vydané směrnice.

Důsledek: finanční náklady na výměnu zámků, postih zaměstnanci za porušení směrnice.

Tab. 7 Ztráta klíčů. (vlastní zpracování)

Kvantifikace rizik	**1.**	**2.**	**3.**	**4.**	**5.**	**Skóre (Ø hodnoty)**	
Možnost výskytu (1 min. – 10 max.)	4	6	5	6	3	**4,8**	x
Dopad (1 min. – 10 max.)	5	7	7	4	8	**6,2**	x
Ocenění rizika = skóre pravděpodobnosti x skóre dopadu							**30**

Rizikový faktor č. 4: neoprávněný přístup k informacím

K neoprávněnému přístupu může dojít především díky nedbalostnímu jednání zaměstnanců, kdy při odchodu z ambulance, recepce nebo pracovny sestry, nedojde k uzamčení kartotéky se zdravotními daty pacientů. Z tohoto důvodu může dojít k neoprávněnému nahlížení do dokumentace popřípadě i k odcizení této dokumentace. K neoprávněnému přístupu k informacím může dojít také v případě neodhlášení uživatele, který pracuje s nemocničním informačním systémem (NIS), ve kterém jsou veškerá zdravotnická data pacientů v elektronické podobě, popř. při sdělení hesla jinému uživateli, kdy může dojít k manipulaci s daty pacientů neoprávněnou osobou.

Důsledek: porušení ZOOÚ, postih za porušení vnitřních předpisů.

Tab. 8 Neoprávněný přístup k informacím. (vlastní zpracování)

Kvantifikace rizik	**1.**	**2.**	**3.**	**4.**	**5.**	**Skóre (Ø hodnoty)**	
Možnost výskytu (1 min. – 10 max.)	4	4	5	4	3	**4**	x
Dopad (1 min. – 10 max.)	7	7	6	7	8	**7**	x
Ocenění rizika = skóre pravděpodobnosti x skóre dopadu							**28**

Rizikový faktor č. 5: neznalost legislativy.

V případě neznalosti legislativy může docházet k porušování povinné mlčenlivosti, ale také k úkonům, které jsou v rozporu s platnými legislativními normami a směrnicemi zdravotnického zařízení. Mezi tyto úkony lze zařadit: poskytování originál ZD neoprávněným osobám, odesílání zdravotních zpráv pacienta bez písemné žádosti oprávněné osoby, v případě nahlížení do ZD nezaznamenání o této skutečnosti, aj.

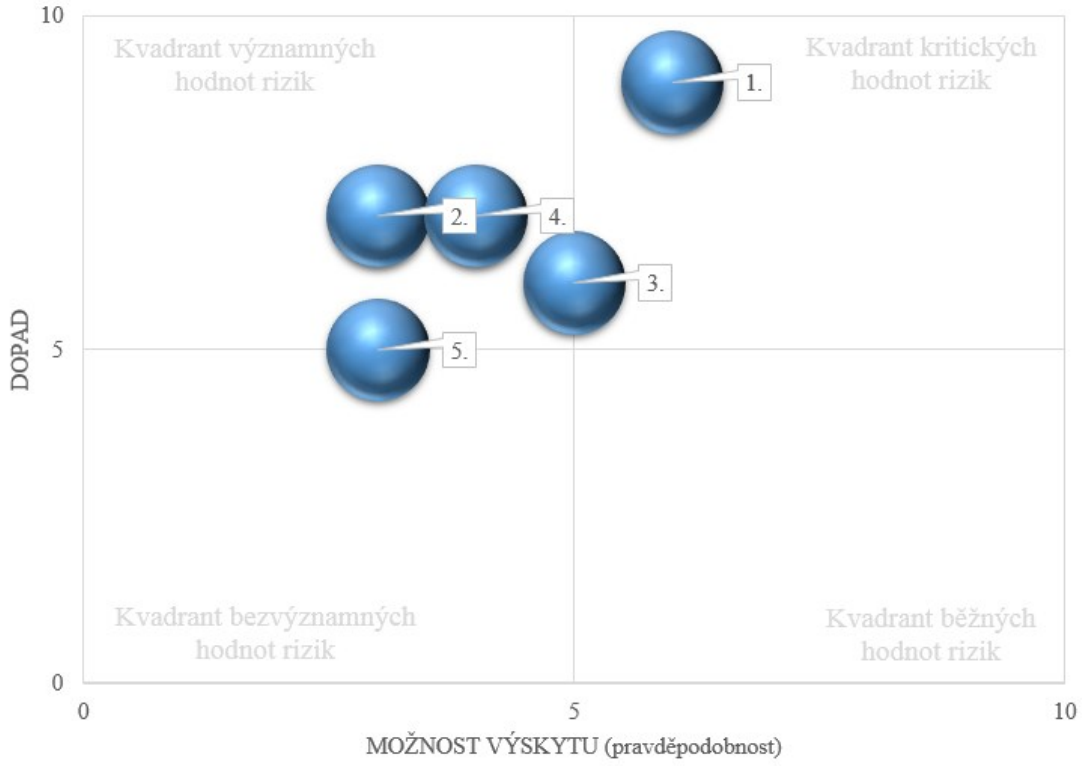
Důsledek: porušení ZOOÚ, postih za porušení vnitřních předpisů.

Tab. 9 Neznalost a nedodržování legislativy. (vlastní zpracování)

Kvantifikace rizik	**1.**	**2.**	**3.**	**4.**	**5.**	**Skóre (Ø hodnoty)**	
Možnost výskytu (1 min. – 10 max.)	2	3	4	3	2	**2,8**	x
Dopad (1 min. – 10 max.)	7	5	4	3	8	**5,4**	x
Ocenění rizika = skóre pravděpodobnosti x skóre dopadu							**15**

12.5 Vyhodnocení rizik

Následující mapa rizik (Obr. 18) na základě skórovací metody rozdělila jednotlivá rizika do jednotlivých kvadrantů dle jejich významnosti pro organizaci.



Obr. 18 Mapa rizik. (vlastní zpracování)

Riziko **ztráty dokumentace** (riziko č. 1), je ohodnoceno jako nejvíce rizikové a nachází se kvadrantu kritických rizik. Na hranici kvadrantu významných a kritických hodnot rizik je riziko ztráty klíčů (riziko č. 3). Další rizika: neoprávněný přístup k informacím (riziko č. 4) a únik citlivých informací (riziko č. 2) jsou v kvadrantu významných rizik.

Jako riziko s nejmenším dopadem na organizaci, bylo vyhodnoceno riziko neznalosti legislativy (riziko č. 5).

12.6 Návrhy opatření

V následujícím seznamu (Tab. 10) jsou uvedeny návrhy na opatření ke snížení rizika. Při detailnějším posouzení rizik a možných návrhů opatření je zásadní problém v zabezpečení ambulancí a pracoven sester kde se nachází nejen ZD, ale i příslušné počítačové vybavení. Další podíl na zvýšeném riziku, je dle mého názoru laxní přístup zdravotnického personálu, kdy si v plné míře neuvědomují daná rizika a spoléhají na toleranci a shovívavost svých nadřízených, ale i pacientů, kteří přišli primárně do zdravotnického zařízení řešit své zdravotní problémy.

Tab. 10 Návrhy opatření ke snížení rizika. (vlastní zpracování)

Pořadové číslo + Rizikový faktor	Návrh opatření
1. Ztráta dokumentace	• Zavedení evidence pohybu ZD • Zvýšení zabezpečení prostorů se ZD
2. Únik citlivých informací	• Aktualizovaný seznam oprávněných osob pro sdělování informací uveden také v NIS • Zvýšení zabezpečení prostor se ZD • Nastavení časového zámku na PC a automatické odhlašování všem uživatelům. • Pravidelné doškolování zaměstnanců při práci s elektronickou ZD • Kontrola a postih za nedodržování směrnic
3. Ztráta klíčů	• Přesná evidence vydaných klíčů a přístupů • Přístupový systém na karty
4. Neoprávněný přístup k informacím	• Přístupový elektronický systém • Zabezpečení kartotéky se ZD zámkem • Nastavení přístupových práv do NIS jen pro oddělení, na kterém zaměstnanec pracuje • Pravidelná aktualizace hesel a přístupů NIS • Pravidelné doškolování zaměstnanců při práci s elektronickou ZD a NIS
5. Neznalost a nedodržování legislativy	• Vydání bezpečnostního desatera • Pravidelné proškolení zaměstnanců vedoucími pracovníky příslušného oddělení

Navrhované opatření vesměs obsahují **doporučení organizačního charakteru** a jejich dodržování souvisí s důsledností vedoucích zaměstnanců při plnění svých povinností a hlavně uvědomění si, že rizika týkající se ochrany citlivých dat pacientů jsou stejně důležitá, jako péče o jejich zdraví. Tyto navrhovaná opatření nevyžadují větší finanční zatížení

pro organizaci a dle mého názoru jsou velmi jednoduše aplikovatelná a lze je zavést bez větších komplikací.

Co se týká návrhu na snížení rizika v podobě **zavedení elektronického přístupového systému**, který by ve větší míře vyřešil základní problematiku zajištění ZD a zvýšení bezpečnosti ochrany citlivých dat pacientů, je již na realizaci časově náročnější. Důležité je také zmínit i nemalé finanční náklady na jeho realizaci. Na druhé stránce v porovnáním s případnými náklady při úniku informací a následné soudní žalobě, je tato částka zanedbatelná.

NÁVRH ŘEŠENÍ: Elektronický přístupový systém

Popis systému

Přístupové systémy (Obr. 19) jsou určeny pro objekty a prostory, kde je třeba zamezit vstupu neoprávněným osobám, případně omezit vstup do určitých částí objektu. Elektronický přístupový systém slouží jako náhrada systémů jednotného klíče. Systém poskytuje i další využití, jako je například:

- možnost nastavení časového oprávnění pro vstup do vybraných prostor;
- evidování pohybů všech osob, včetně pokusů o neoprávněné vstupy;
- signalizace hlídaných vstupů (násilné vniknutí, nezavření dveří);
- možnost využití docházkového systému, přístup na parkoviště.

Jak systém funguje

Vstupní místa přístupového systému jsou vybavena čtečkami a elektromechanickým zařízením pro blokování vstupu (elektrické zámky). Odblokování vstupního místa proběhne na základě vyhodnocení oprávnění, nastaveného v obslužném softwaru. Vstupní místa lze ovládat jednostranně i oboustranně dle potřeb provozu. Pomocí dveřních snímačů lze monitorovat a signalizovat stav dveří. [32]

Informace o všech událostech v systému se přenášejí do databáze v počítači, kde je monitoruje a zpracovává přístupový software. Výsledkem jsou přehledy o tom, kdo vstoupil, kdy, kam a na jakou dobu. [32]

Obr. 19 Přístupový systém. [32]

Požadované parametry

Pro zpracování orientační kalkulace byla odeslána poptávka s těmito požadavky (zpracováno za jedno vybrané oddělení):

- přístupy pro 50 zaměstnanců;
- 25 dveří s možností individuálního nastavení a možností časového zámku;
- Přesnou evidenci vstupů (pro případ neoprávněného vstupu, ztráty);
- Přístup přes biometrickou identifikací (otisk prstu), popř. kartu.

Cenová kalkulace

Pro cenovou kalkulaci jsem oslovila čtyři firmy, které se zaváděním přístupových systémů do organizací zabývají. S doručených nabídek jsem vybrala následující (tab. 11), která poskytuje vstupní přehled, v jakých cenových relacích se zavedení systému pohybuje. Samozřejmě, že pro zavedení tohoto systému do celého zdravotnického zařízení, by se cena za realizaci pohybovala v jiném rozpětí. Pro orientační kalkulaci byla nabídnuta i varianta s čtečkou otisku prstu, což by byla vzhledem k nezaměnitelné identifikaci ideální varianta. Cena za tuto variantu byla o 340 000 Kč vyšší.

Tab. 11 Cenová kalkulace přístupového systému. (vlastní zdroj)

Název sortimentu	**Počet ks**	**Cena celkem**
Centrální řídící jednotka	1	18 900 Kč
Modul směrnicová čtečka, antivandal, relé	25	88 750 Kč
Akumulátor	1	1 150 Kč
Program PŘÍSTUPY, SLUŽBA, komunikační plánovač	1 + 1	9 500 Kč
ID karta	50	2 950 Kč
Personifikátor (čtečka)	1	1 850 Kč
CELKOVÁ CENA (Kč bez DPH)		**123 100 Kč**

V případě dodávky včetně instalace bude zakázka účtována s 0 % DHP.

Tyto přístupové systémy jsou běžně zaváděny do organizací s různým oborem zaměření. V některých zdravotnických zařízení jsou již standardním vybavením. Dle mého názoru velkou výhodou těchto systémů je jejich široké využití, kterého by se dalo využít i v této organizaci.

13 ZÁVĚR

Problematice ochrany osobních údajů je již mnoho let věnována značná pozornost, přesto se ještě dnes překvapivě často setkáváme s tím, že si lékaři dostatečně neuvědomují, jak velké riziko může znamenat podceňování ochrany citlivých dat pacientů. Neustále slýcháváme, že jejich hlavním posláním je léčit pacienty. Je nezbytné si také uvědomit, že rozvojem informačních technologií, propojeností systémů a zvýšeným rizikem úniku těchto informací, je nezbytné chránit nejen sebe, dobré jméno zdravotnického zařízení, ale hlavně práva pacientů, kteří s důvěrou přichází k lékaři do zdravotnického zařízení.

Základem teoretické části bylo vymezení pojmů a legislativy související s problematikou. Část je také věnovaná bezpečnosti osobních údajů s uvedením práv a povinnosti všech, kteří s těmito daty jakkoliv nakládají. Jednotlivé rozdělení hrozeb, možných dopadů a vzájemné působení všech prvků informační bezpečnosti řeší samostatná kapitola. Závěrečná kapitola s názvem „Organizační zabezpečení informací“, popisuje jednotlivé etapy zavádění informační bezpečnosti v organizaci.

Úvodem praktické části je obecně definován systém zdravotnictví v České republice, popsána zdravotnická dokumentace, která je hlavním zdrojem citlivých údajů pacientů, související legislativa a přehled informačních systémů ve zdravotnictví. Po definování prostředí zdravotnického zařízení, je následně provedená analýza zaměřena na ochranu citlivých dat pacientů se zaměřením za ZD. Výsledky analýzy obsahují doporučení, které se převážně týkají zlepšení organizačního zabezpečení. Jak je konstatováno již v praktické části ukázalo se, že největším zdrojem rizika je lidský faktor. Jako stěžejní a dle mého názoru velmi přínosným opatřením pro snížení vyhodnocených rizik je zavedení elektronického přístupového systému, jejichž výhody a možnosti dalšího využití jsou popsány v práci. Za zavedení systému na jedno oddělení, na kterém se pohybuje cca padesát zaměstnanců a je nutné zabezpečit 25 přístupových míst (dveří od ambulancí, lůžkového oddělení či archivu) je orientační kalkulace 123 100 Kč. Pro komplexní zabezpečení přístupů v celém zdravotnickém zařízení by cena samozřejmě byla několikanásobně vyšší. Ale vzhledem k tomu, že rizika spojená s únikem informací a tím související nedodržení zákona o ochraně osobních údajů, kde hrozí při porušení nemalé sankce a ztráta důvěryhodnosti organizace, je tato částka zanedbatelná.

Výsledky práce a včetně návrhů na snížení zjištěných rizik, byly předány pracovníkům, kteří jsou v organizaci odpovědni za informační a organizační zabezpečení.

SEZNAM POUŽITÉ LITERATURY

[1] ČERMÁK, Miroslav. *Řízení informačních rizik v praxi*. V Tribunu EU vyd. 1. Brno: Tribun EU, 2009, 134 s. Knihovnicka.cz. ISBN 978-80-7399-731-1.

[2] POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005, 309 s. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-868-9838-5.

[3] DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011, 286 s. ISBN 9788074310508.

[4] MATOUŠOVÁ, Miroslava a Ladislav HEJLÍK. *Osobní údaje a jejich ochrana.* 2., dopl. a aktualiz. vyd. Praha: ASPI, 2008, 455 s. ISBN 978-80-7357-322-5.

[5] ZEHLOVÁ, Veronika. *Správněprávní aspekty ochrany osobních údajů*. 2009. Dostupné také z: http://is.muni.cz/th/108011/pravf_m/diplomka.pdf. Diplomová práce. Právnická fakulta Masarykovy univerzity.

[6] ČESKO. Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. In: *Sbírka zákonů ČR*. 2000. Dostupné také z: http://www.zakonyprolidi.cz/cs/2000-101

[7] MATES, Pavel. *Ochrana osobních údajů*. Vyd. 1. Praha: Karolinum, 2002, 73 s. ISBN 8024604698.

[8] NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář*. Vyd. 1. Praha: Wolters Kluwer, 2014, xx, 484 s. Komentáře (Wolters Kluwer ČR). ISBN 9788074786655.

[9] MACH, Jan. *Medicína a právo*. Vyd. 1. V Praze: C.H. Beck, 2006, xiii, 257 s. Beckova edice ABC. ISBN 80-7179-810-x

[10] Co jsou a co nejsou osobní údaje, jak jsou chráněny a jak se my sami můžeme starat o jejich ochranu. *Parlamentní listy* [online]. [cit. 2016-01-03]. Dostupné z: http://www.parlamentnilisty.cz/arena/monitor/Co-jsou-a-co-nejsou-osobni-udaje-jak-jsou-chraneny-a-jak-se-my-sami-muzeme-starat-o-jejich-ochranu-300971.

[11] Sankce za nakládání s osobními údaji v rozporu se zákonem. In: *Ochrana osobních údajů* [online]. 2014 [cit. 2016-01-31]. Dostupné z: http://www.oou.cz/zacinamesochranou/sankce

[12] Kybernetická bezpečnost. In: *Linux Servises* [online]. [cit. 2016-01-31]. Dostupné z: https://www.linuxservices.cz/kyberneticka-bezpecnost

[13] BOŘÁNEK, Roman. Kybernetická bezpečnost: O čem je nový zákon. In: root.cz [online]. 2015 [cit. 2016-01-31]. Dostupné z: http://www.root.cz/clanky/kyberneticka-bezpecnost-o-cem-je-novy-zakon/

[14] Kybernetická bezpečnost. In: *T-soft* [online]. 2014 [cit. 2016-01-31]. Dostupní z: http://www.tsoft.cz/bezpecnost-kyberneticky-zakon/

[15] ČERMÁK, Miroslav. Informační bezpečnost vs. kybernetická bezpečnost. In: *Clever and Smart* [online]. 2014 [cit. 2016-01-31]. Dostupné z: http://www.cleverandsmart.cz/information-security-vs-cybersecurity/

[16] BŘICHÁČEK, Zdeněk. *Audit informační bezpečnosti - informační bezpečnost* [online]. In:. [cit. 2016-02-15]. Dostupné z: http://blog.brichacek.net/audit-informacni-bezpecnosti-informacni-bezpecnost/

[17] PŘIBYL, Tomáš. Jak na organizační bezpečnost. In: *ICT Security* [online]. 2010 [cit. 2016-01-31]. Dostupné z: http://www.ictsecurity.cz/odborne-clanky/jak-na-organizacni-bezpecnost.html

[18] Management mania: *Řízení rizik (Risk management)* [online]. [cit. 2016-04-30]. Dostupné z: https://managementmania.com/cs/rizeni-rizik

[19] DOLEŽAL, Jan, Pavel MÁCHAL a Branislav LACKO. *Projektový management podle IPMA*. 1. vyd. Praha: Grada, 2009. Expert (Grada). ISBN 978-80-247-2848-3.

[20] ČESKO. Předpis č. 98/2012 Sb., vyhláška o zdravotnické dokumentaci a o změně některých zákonů. In: Sbírka zákonů ČR. 2012. Dostupné také z: http://www.zakonyprolidi.cz/cs/2012-98

[21] ŠNÉDAR, Libor. Základy zdravotnického práva: s příklady a otázkami. 1. vyd. Praha: LexisNexis CZ, 2008. Studijní texty (LexisNexis CZ). ISBN 978-80-86920-21-4.

[22] Zdravotnictví v ČR 2013 ve statistických údajích. Praha, 2014. ISBN 978-80-7472-101-4. ISSN 0862-5883. Dostupné také z: http://www.uzis.cz/katalog/kardexy/zdravotnictvi-cr-ve-statistickych-udajich

[23] *Ministerstvo zdravotnictví České republiky: Druhy zdravotní péče* [online]. [cit. 2016-04-30]. Dostupné z: http://www.mzcr.cz/Cizinci/obsah/druhy-zdravotni-pece_2627_22.html

[24] POLICAR, Radek. Zdravotnická dokumentace v praxi. 1. vyd. Praha: Grada, 2010, 223 s. ISBN 9788024723587.

[25] MACH, Jan. Univerzita medicínského práva. 1. vyd. Praha: Grada, 2013. ISBN 978-80-247-5113-9.

[26] ČESKO. Předpis č. 98/2012 Sb., vyhláška o zdravotnické dokumentaci a o změně některých zákonů. In: Sbírka zákonů ČR. 2012. Dostupné také z: http://www.zakonyprolidi.cz/cs/2012-98

[27] MACH, Jan. Medicína a právo. Vyd. 1. V Praze: C.H. Beck, 2006, xiii, 257 s. Beckova edice ABC. ISBN 80-7179-810-x.

[28] VALENTOVÁ, Renata. Vedení spisové služby ve FN Brno zaměřené na zdravotnickou dokumentaci. Dostupné také z: http://is.muni.cz/th/243936/ff_b/. Bakalářská práce. Filozofická fakulta Masarykovy univerzity.

[29] UHEREK, Pavel. Povinná mlčenlivost zdravotnických pracovníků: komplexní rozbor aktuální právní úpravy: výjimky a právní odpovědnost: řešení sporných či komplikovaných případů z praxe: praktickou součástí jsou zpracované vzory formulářů. 1. vyd. Praha: Grada, 2008, 182 s. Právo pro praxi. ISBN 9788024726588.

[30] PŘIBÍK, Vladimír. Elektronická zdravotnická dokumentace, registry a nemocniční informační systémy. In: SlidePlayer [online]. [cit. 2016-03-29]. Dostupné z: http://slideplayer.cz/slide/2453625/

[31] Kronika události 2004: Z pozoruhodnosti novojičínského života. In: Nový Jičín [online]. [cit. 2016-03-31]. Dostupné z: http://www.novy-jicin.cz/customers/novy-jicin/ftp/File/kronika_udalosti/kronika2004prava.pdf

[32] *ACS line: Přístupové systémy* [online]. [cit. 2016-04-30]. Dostupné z: http://www.acsline.cz/cs/pristupovy-system

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

Aj.	A jiné
Apod.	A podobně
ARO	Anesteziologicko-resuscitační oddělení
Atd.	A tak dále
CT	Počítačová tomografie
Č.	Číslo
DPH	Daň s přidané hodnoty
IPVZ	Institut postgraduálního vzdělávání ve zdravotnictví
IS/IT	Informační systém / informační a komunikační technologie
ISO/IEC	Mezinárodní organizace pro normalizaci
KHS	Krajská hygienická stanice
KSRZIS	Koordinační středisko pro zdravotnické informační systémy
KÚ	Krajský úřad
MOJIP	Mezioborová jednotka intenzivní péče
MRI	Magnetická rezonance
MZ ČR	Ministerstvo zdravotnictví České republiky
Např.	Například
NATO	Severoatlantická aliance
NBÚ	Národní bezpečnostní úřad
NIS	Nemocniční informační systém
NLK	Národní lékařská knihovna
Obr.	Obrázek
OIT	Oddělení informačních technologií
ORL	Otorhinolaryngologické oddělení

RDG	Radiodiagnostika
Resp.	Respektive
SZÚ	Státní zdravotní ústav
Tab.	Tabulka
THP	Technicko-hospodářský pracovník
Tzn.	To znamená
Tzv.	Tak zvaně
ÚOOÚ	Úřad na ochranu osobních údajů
ÚZIS	Ústav zdravotnických informací a statistiky ČR
Vs.	Versus
VZP	Všeobecná zdravotní pojišťovna
ZOOÚ	Zákon o ochraně osobních údajů
ZP	Zdravotnický pracovník
ZPZL	Zákon o zdraví a péči lidu
ZZS	Zákon o zdravotních službách

SEZNAM OBRÁZKŮ

SEZNAM TABULEK