Zdravotně sociální fakulta
Faculty of Health and Social Sciences

Jihočeská univerzita v Českých Budějovicích
University of South Bohemia in České Budějovice

Ochrana zdravotnických zařízení důležitých z pohledu ochrany obyvatelstva

DIPLOMOVÁ PRÁCE

Studijní program:

OCHRANA OBYVATELSTVA

Autor práce: Bc. Tomáš Naar

Vedoucí práce Ing. Lenka Michalcová, Ph.D.

České Budějovice, 2021

Prohlášení

Prohlašuji, že svoji diplomovou práci s názvem Ochrana zdravotnických zařízení důležitých z pohledu ochrany obyvatelstva, jsem vypracoval samostatně, pouze s použitím pramenů v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své diplomové práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby diplomové práce. Rovněž souhlasím s porovnáním textu mé diplomové práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích dne 10.5 2021 .....

podpis

Poděkování

Tímto bych rád poděkoval vedoucí mé diplomové práce, paní Ing. Lence Michalcové, Ph. D za všestrannou pomoc, množství cenných a inspirativních rad, podnětů, doporučení, připomínek a zároveň za trpělivost při konzultacích poskytnutých ke zpracování této práce.

Ochrana zdravotnických zařízení důležitých z pohledu ochrany obyvatelstva

Abstrakt

Bezpečnostní situace v celém světě i Evropě se během posledních let zhoršuje. Nejrůznější druhy útoků na nejrůznější cíle jsou běžně na denním pořádku. Výjimkou u těchto útoků nejsou ani zdravotnická zařízení, jejich personál i pacienti. V minulosti se objevilo mnoho útoků, jak v České republice, tak i v zahraničí. Navzdory této stoupající tendenci nelze říct, že stoupá i úroveň zabezpečení těchto objektů. Proto si tato diplomová práce dala za cíl zjistit, na jaké úrovni jsou momentálně bezpečnostní opatření v rámci fyzické ochrany zdravotnických zařízení. Dále popisuje potencionální rizika, kterým mohou být zdravotnická zařízení vystavena.

Pro zjištění těchto informací byla vydefinována potencionální rizika na základě Analýzy hrozeb České republiky. Aktuální stav fyzické ochrany byl hodnocen na nejmenovaném zdravotnickém zařízení a podle výsledků pak byla zhodnocena kvalita zabezpečení všech zdravotnických zařízení.

Pro praktickou část diplomové práce byla zvolena metoda analýzy, která měla za cil zjistit odpověď na dvě výzkumné otázky uvedené v kapitole číslo 2. Stanovený postup řešení úkolu zahrnuje jak metodu analýzy, tak i syntézy. Výstupem této diplomové práce je zjištění, že fyzická ochrana zdravotnických zařízení není v současné době dostatečná. Zároveň tato diplomová práce stanovila slabá místa v oblasti bezpečnosti a jejich náprava by mohla výrazně navýšit celkovou úroveň zabezpečení zdravotnického zařízení. Výzkum v praktické části jako nejslabší místa ve zdravotnickém zařízení zařadil: Ambulantní čekárny, jednotky intenzivní péče, urgentní příjem, lékárny a stravovací prostory. Dále je zde zhodnoceno zabezpečení celého areálu zdravotnického zařízení. Pro všechny tyto objekty diplomová práce navrhuje konkrétní řešení, které je zapotřebí realizovat pro adekvátní zajištění bezpočetnosti pro osoby nacházející ve zdravotnickém zařízení.

Klíčová slova

Ochrana obyvatelstva, fyzická ochrana, zdravotnické zařízení

Protection of medical facilities important for population protection

Abstract

The security situation worldwide and in Europe has deteriorated in recent years. Many types of attacks on different targets are common every day. Medical facilities, their staff and patients are no exception to these attacks.

In the past, there have been many attacks in Czech Republic, but it cannot be said that the level of security of these objects is rising. Therefore, this thesis decides to find out on what level are currently the safety measures in the physical protection of medical facilities. Thesis also describes the potential risks to which healthcare facilities may be exposed. To determine this information, potential risks were determined based on the Threat Analysis of the Czech Republic. The current state of physical protection was assessed at an unnamed medical facility according to the results, and the quality of security of all medical facilities was assessed.

For the practical part of the diploma thesis, the method of analysis was chosen. These methods aimed to find out the answer to the two research questions listed in Chapter 2. The procedure for solving the task includes both the method of analysis and synthesis.

The output of this thesis is the finding that the physical protection of medical facilities is currently insufficient. At the same time, this thesis identified weaknesses in the field of safety and their correction could significantly increase the overall level of security of the medical facility. In the practical part, the research included the weakest places in the medical facility: Outpatient waiting rooms, intensive care units, emergency admission, pharmacies, and dining areas. Furthermore, the security of the entire area of the medical facility is evaluated here. For all these objects, the thesis proposes a specific solution that needs to be implemented to ensure the safety of persons in a medical facility

Key words

Protection of Population, Physical protection, Hospital

OBSAH

1 ÚVOD

Pro tuto diplomovou práci bylo zvoleno téma zabývající se fyzickou ochranou zdravotnických zařízení v České republice. Tato diplomová práce s názvem Ochrana zdravotnických zařízení důležitých z pohledu ochrany obyvatelstva se zabývá technickým zabezpečením zdravotnických zařízení před nejrůznějšími druhy fyzického napadení. Fyzická ochrana je nepříliš známý pojem a doposud nebyl legislativně definován. Zabývá se zabezpečením vstupů do areálu, ochranou samotného areálu před vniknutím a poškozením. Dále například monitorací objektů skrze kamerový systém nebo dohledem nad pohybem osob skrze vyškolené pracovníky fyzické ostrahy. Jejich hlavním úkolem je zneškodnit jakéhokoliv útočníka, který by mohl způsobit poškození na zdraví jak personálu, tak i pacientů.

Za posledních několik let Ministerstvo zdravotnictví eviduje desítky potvrzených útoků ve zdravotnických zařízeních. Jeden z nich, ve Fakultní nemocnici Ostrava, je kategorizován už jako útok teroristický. Ze statistik je dále patrné, že frekvence útoků se v této oblasti zvyšuje. Sám autor je zaměstnanec jednoho nejmenovaného zdravotnického zařízení. Toto vybrané téma je důležité z toho důvodu, že nemocnice má být místem, kde se bolest a utrpení eliminuje, a v žádném případě by neměla být místem dalšího neštěstí. Bohužel počty napadených zdravotnických zařízení stále rostou, a proto je potřeba, aby byla zdravotnická zařízení na tyto situace plně připravena, a v případě, že nastanou, dokázat adekvátně reagovat. Hlavním pilířem ochrany zdravotnického zařízení je kvalitní preventivní plán. Využití represivních složek by mělo být vždy až na druhém místě jako záložní plán pro řešení vzniklých problémů. S bezpečností zdravotnických zařízení je v poslední době úzce spojená bezpečnost kybernetická. Problematika kybernetických útoků a ztráty citlivých dat ale není součástí této diplomové práce

V této diplomové práci bude nejprve sumarizováno celé odvětví fyzické ochrany, její rozdělení, jednotlivé bezpečnostní prvky a jejich možné využití v zabezpečení zdravotnického zařízení. Dále bude uvedena základní legislativa a bezpečnostní normy, jejichž znalost je stěžejní pro tvorbu kvalitního konceptu fyzické ochrany zdravotnického zařízení. Ve druhé části budou definovány potencionální hrozby, kterým mohou zdravotnická zařízení čelit. Dále bude zhodnocena celková stávající úroveň fyzické ochrany u zdravotnických zařízení a na základě této analýzy budou definovány návrhy na zlepšení bezpečnosti v jednotlivých oblastech fyzické ochrany. Bude zde také navrhnuta případná koncepce, která centrálně nastaví minimální úroveň fyzické ochrany ve všech zdravotnických zařízeních.

2 TEORETICKÁ ČÁST

Teoretická část diplomové práce shrnuje všechny hlavní teoretická technická a legislativní odvětví, která jsou stěžejní pro shrnutí problematiky fyzické ochrany zdravotnických zařízení.

2.1 Úvod do problematiky

Napadení zdravotnických zařízení se stalo v posledních letech hojně diskutovaným tématem, jelikož se odehrálo napříč Českou republikou několik závažných událostí. Jednotlivé útoky se liší případ od případu, jak zvoleným druhem útoku, tak i psychickým či materiálním vybavením útočníka. Je potřeba nezapomínat a považovat za reálnou hrozbu útok nejen zvenčí ale také napadení uvnitř zdravotnického zařízení, které realizuje útočník z řad pacientů. Proto je skrze interní nařízení nutné předejít jak napadení personálu pacientem, tak i zamezit konfliktu kvalitní intervencí například mezi jednotlivými pacienty. Právě tyto případy se začaly vyskytovat se stoupající tendencí a vyžádaly si i oběti na životech.

Případy vážnějšího typu napadení ostatních pacientů nebo personálu nemocnic nejsou v ČR tak ojedinělé, jak by se mohlo zdát. Pravděpodobně nejvíce drastickým případem v moderních dějinách je střelba v čekárně polikliniky ostravské fakultní nemocnice 10. prosince loňského roku. Zde mladý střelec sedm lidí zabil, dva zranil a poté spáchal sebevraždu dříve, než ho zásahová jednotka stihla dopadnout. Další případ se stal v březnu ve Fakultní nemocnici Královské Vinohrady, kde pacient postřelil dva lidi, jeden z nich pak bohužel svým zraněním podlehl. K dalšímu napadení došlo na hematologické klinice, kde střílel čtyřiasedmdesátiletý pacient kvůli osobnímu konfliktu s ostatními pacienty na nemocničním pokoji. Střelec po činu odmítl vypovídat a koncem dubna obviněný senior zemřel v pankrácké věznici. V lednu 2010 šestatřicetiletý muž hospitalizovaný na psychiatrické klinice v Praze na Karlově kvůli těžkému maniodepresivnímu stavu brutálně zbil a následně usmrtil jiného pacienta. Soud mu později nařídil ochrannou ústavní léčbu. (Vohlídal, 2020)

Smutným koncem skončil případ útočníka, kdy v listopadu 2015 ve Fakultní nemocnici v Olomouci psychicky nemocný muž surově napadl sanitáře. Přivolaní policisté použili pro zpacifikování útočníka paralyzér, ale tento zásah psychicky nemocný pacient nezvládl. Mezi první větší incidenty patří ten ze září roku 2005, kdy podnapilý muž zaútočil na přivolané policisty v nemocnici v Táboře. (Vohlídal, 2020)

Jednomu z nich vzal služební pistoli a šestkrát z ní vystřelil. Naštěstí nedošlo ke zranění nikoho z přítomných. Bez vážnějších zranění skončily pak i dva další incidenty z roku 2014, ve kterých hrála roli střelná zbraň. Nejprve v červnu střílel pacient ve FN Ostrava, který zbraň odcizil pracovníkovi bezpečnostní služby, podruhé pak v září „jen" vyhrožoval se zbraní v ruce opilý muž v pražské střešovické nemocnici (Vohlídal, 2020).

Ve 21. století čelí nemocnice ještě jedné zásadní hrozbě, která by se mohla zdát jako zcela banální. Ještě pár let zpět by toto riziko nikdo nepovažoval za reálný problém. Toto riziko představují kybernetické útoky na informační systém nemocnic a s tím spojené technologické sítě, které mohou přímo ohrozit pacienty poškozením přístrojů nebo v širší rovině vyřazením celé nemocnice z provozu na několik hodin až dní, nehledě na ekonomické dopady útoků, které se mohou vyšplhat až k desítkám milionů korun. V roce 2019 hackeři napadli více jak pětinu českých nemocnic (Čambora, 2020). Specialista na kybernetickou bezpečnost z poradenské firmy BDO, Martin Hořický, uvádí, že mezi nejhorší útoky patří ty s vyděračským programem, který většinou přichází do organizace skrze email, jako běžná příloha. Po otevření zaměstnancem dojde k aktivaci, která může mít za následek ochromení celé nemocnice. Nefungují přístroje, nefunguje přenos informací mezi jednotlivými pracovišti a lékaři nemohou ani otevřít karty svých pacientů. Pokud je to aspoň trochu možné, je zapotřebí odložit operace. Riziková je také ztráta obrovského množství citlivých osobních dat a jejich potencionální prodej na černém trhu. Hlavní příčinu tohoto problému vidí Hořický v zastaralém softwaru, nedostatečném financování a také v absenci odborných kapacit pro správu těchto informačních systémů.

2.2 **Popis zdravotnického zařízení**

Podle zákona č. 372/2011 se jedná o zařízení poskytující operativní a ošetřovatelskou péči na odděleních urgentního příjmu a lůžkovém oddělení anesteziologicko-resuscitačního oddělení, které zajišťují hlavní cíl zdravotnického zařízení. Dále poskytuje akutní péče na oborových jednotkách intenzivní péče, které zajišťují odvrácení celkového zhoršení stavu pacienta. Základním pilířem péče ve zdravotnických zařízeních jsou standartní lůžková oddělení, která přijímají pacienty, jejichž stav vyžaduje hospitalizaci, ale zdravotní stav nevyžaduje hospitalizaci na odděleních intenzivní péče. Poslední složkou jsou pak jednotky zajištující konzultační nebo ambulantní péči, do které pacienti sami pouze docházejí. (Část 2 zákona č. 372/2011).

Dále lze zdravotnická zařízení rozdělit podle typu, a to na ZZ prvního kontaktu, kam spadá praktický lékař, zubní lékař a lékařská služba první pomoci. Dále pak výše zmíněné všechny druhy ambulantní péče. Zvláštními druhy ambulantní péče jsou protialkoholní a protitoxikomanické záchytné stanice. Krizová střediska, kde dochází k poskytování diagnostické a léčebné péče u pacientů trpících akutním psychickým stavem.

Hlavním typem jsou hospitalizační zdravotnické zařízení. Tato zařízení rozdělujeme podle úrovně poskytované péče, která záleží na materiálních, technických a kapacitních možnostech, a to jak z pohledu personálu, tak počtu hospitalizovaných pacientů. (Fořtl, 2003)

Obvodní zdravotní středisko

- Spádová oblast: 4-10 000 obyvatel.
- Pracoviště: praktický lékař, zubní lékař, pediatr, gynekolog.
- Hygienická stanice není zřizována pro oblast tak malého rozsahu.

Nemocnice I. typu

- Spádová oblast: 50 000 obyvatel, počet lůžek 300-500.
- Ambulantní pracoviště: interní, chirurgické, gynekologické, dětské, urgentní příjem.
- Léčený komplex: centrální příjem, hematologická a biochemická laboratoř, centrální operační sály, centrální sterilizace, radiodiagnostické oddělení, rehabilitace.
- Lůžkové oddělení: interní, chirurgické, gynekologicko-porodnické, dětské oddělení.
- Nemocnice prvního typu poskytují ošetřovatelskou lůžkovou péči nepřerušeně, a to podle potřeb spádové oblasti. Musí mít zřízenou jednotku intenzivní péče a zajišťovat ošetřovatelskou péči v chirurgických a interních oborech. (Fořtl, 2003)

Nemocnice II. typu

- Spádovost: 200 000 obyvatel počet lůžek 600-900.
- Ambulantní pracoviště: interní, chirurgické, gynekologické, kožní, ORL, ortopedie, urologie, LSPP, příp. infekční odd.
- Léčebný komplex: centrální příjem, hematologická a biochemická laboratoř, centrální operační sály, centrální sterilizace, radiodiagnostické oddělení, rehabilitace, transfúzní oddělení.

- Lůžkové oddělení: chirurgické, interní, neurologické, gynekologicko-porodnické, anesteziologicko-resuscitační oddělení, LSPP, ortopedické, plicní, kožní, urologické, ORL, příp. infekční.
- Okresní hygienicko-epidemiologická stanice II. stupně: hygiena, epidemiologie a mikrobiologie. (Fořtl, 2003)

Nemocnice druhého typu jsou povinny poskytovat nepřerušeně ošetřovatelskou péči v oblasti anesteziologie a resuscitace i v dalších základních oborech (chirurgie, interna, neurologie…). Nemocnice provozuje také oddělení včasné léčebné rehabilitace, a to nejčastěji lůžkovým způsobem. Dále poskytuje neustále základní a specializované diagnostické procedury ke zjištění příčiny nemoci pacienta. Nemocnice dále musí provozovat krevní banku nebo alespoň odběrové místo. (Fořtl, 2003)

Nemocnice III. typu (obvykle nemocnice fakultní)

Standardně rozdělena na trakt pro dospělé a děti. To se týká jak části ambulantní, tak lůžkové

- Ambulantní pracoviště: viz II typ + některé zvláště specializované oddělní. V případě, že se jedná o nemocnici fakultní, tak ta standardně bývá rozdělená na konkrétní kliniky pro dané obory, nikoliv běžná oddělení.
- Léčebný komplex: centrální příjem, hematologická a biochemická laboratoř, centrální operační sály, centrální sterilizace, radiodiagnostické oddělení, rehabilitace, transfúzní oddělení, laboratoř vyšší nervové činnosti, alergoimunologie, histologie, oddělení patologicko-anatomické a soudního lékařství.
- Lůžkové oddělení: Chirurgické, interní, neurologické, gynekologicko-porodnické, anesteziologicko-resuscitační oddělení, kardiologie, neurochirurgie, popáleninové centrum, LSPP, ortopedické, plicní, hrudní chirurgie, kožní, urologické, ORL, příp. infekční. (Fořtl, 2003)

Nemocnice III. typu zajišťují provoz nepřetržitě stejně jako nemocnice II. typu. Liší se od sebe jen rozsahem kapacity, a to jak v případě standardních oddělení, tak i v rámci jednotlivých specializovaných pracovišť. (Fořtl, 2003)

Nedílnou součástí jsou dále lékárny. Ty jsou taktéž rozděleny na I. až III. typ podle zdravotnického zařízení, ke kterému náleží. Odlišnou kategorii pak tvoří soukromé výdejny léků a zdravotnického materiálu. Lékárny zajištují uchování, výdej i prodej medikamentů a ostatních zdravotnických prostředků. Zdravotnické zařízení zahrnuje také všechny specializované laboratoře, zdravotní dopravu nemocných (ZZS, LZS, DRNR.), hygienickou službu a všechna lázeňská zdravotnická zařízení. (Fořtl, 2003)

2.3 Činnost zdravotnického zařízení během krizové situace

Ochrana veřejného zdraví je dle zákona č. 258/2000 Sb., o ochraně veřejného zdraví souhrn činností a opatření k vytváření a ochraně zdravých životních a pracovních podmínek. Ochrana veřejného zdraví by také měla zabránit šíření infekčních a hromadně se vyskytujících onemocnění, ohrožení zdraví v souvislosti s vykonávanou prací, vzniku nemocí souvisejících s prací a jiných významných poruch zdraví a dozoru nad jejich zachováním. Ohrožení veřejného zdraví je stav, při kterém je obyvatelstvo nebo jeho část vystaveno nebezpečí, z něhož míra zátěže rizikovými faktory přírodních, životních nebo pracovních podmínek překračuje obecně přijatelnou úroveň a představuje významné riziko poškození zdraví. (Zákon č. 258/2000 Sb.)

Mezi orgány ochrany veřejného zdraví patří krajské hygienické stanice se svými územními pracovišti a Ministerstvo zdravotnictví jako zřizovatel. Mezi orgány ochrany veřejného zdraví se ve své působnosti řadí také Ministerstvo vnitra, Ministerstvo obrany, Ministerstvo dopravy, Ministerstvo pro místní rozvoj, Ministerstvo životního prostředí a krajské úřady. Orgány ochrany veřejného zdraví plní z pohledu krizového řízení zásadní úlohu při epidemickém výskytu infekčních nemocí. Pro svou připravenost pro řešení takových situací krajská hygienická stanice zpracovává krizový plán. (Šín, 2017)

V případě krizové připravenosti poskytovatelů zdravotních služeb hrají stěžejní úlohu jejich traumatologické plány. V případě prvků kritické infrastruktury jsou významné i plány krizové připravenosti prvků kritické infrastruktury. V těchto plánech jsou identifikovány možné ohrožení funkce a stability prvků kritické infrastruktury a stanovena opatření pro jejich ochranu. Pro zajištění krizové připravenosti poskytovatelé zdravotnické záchranné služby zřizují pracoviště krizové připravenosti, které zpracovává návrh traumatologického plánu, včetně jeho aktualizací a změn. Následně ho předkládá hejtmanovi kraje. Poskytovatelé jednodenní a lůžkové zdravotní péče musí zpracovávat traumatologický plán.

Návrh plánu a jeho aktualizace musí projednat se správním orgánem, který je místně příslušný k udělení oprávnění poskytování zdravotních služeb. V případě fakultních nemocnic se návrh plánu a jeho aktualizace projednává přímo s Ministerstvem zdravotnictví. (Šín, 2017)

Reakce orgánu krizového řízení ve zdravotnictví se řídí podle zákona č. 240/2000 Sb., o krizovém řízení. Stanovuje působnost a pravomoc státních orgánů a orgánů územních samosprávných celků, práva a povinnosti právnických a fyzických osob při přípravě na krizové situace, při jejich řešení a při ochraně kritické infrastruktury. Krizovým řízením se podle tohoto zákona rozumí souhrn řídících činností orgánů krizového řízení zaměřených na analýzu a vyhodnocení bezpečnostních rizik a plánování. Dále také organizování, realizace a kontrola činností prováděných v souvislosti s přípravou na krizové situace a jejich řešení nebo ochranou kritické infrastruktury. (Zákon č. 240/2000 Sb.)

Ministerstvo zdravotnictví jako orgán krizového řízení zajišťuje v oblasti své působnosti (§ 10 zákona č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky) připravenost na řešení krizových situací. Pro tyto účely má zřízeno pracoviště krizového řízení, krizový štáb, který funguje jako pracovní orgán, připravuje se na krizové situace a zpracovává krizový plán. Dále Ministerstvo zdravotnictví (§8 zákona č. 239/2000 Sb.) na vyžádání kraje koordinuje činnost poskytovatele zdravotnické záchranné služby i poskytovatele zdravotnické dopravní služby a přepravy pacientů neodkladné péče. (MZČR, 2020)

Při koordinaci je poskytovatel zdravotnické záchranné služby, poskytovatel zdravotnické dopravní služby a přepravy pacientů neodkladné péče povinen uposlechnout pokynů Ministerstva zdravotnictví ČR. Ministerstvo zdravotnictví odpovídá v okruhu své působnosti za výběr a metodické řízení přípravy zdravotnických pracovníků a za výběr prostředků pro mezinárodní záchranné operace a poskytování humanitární pomoci do zahraničí. (MZČR, 2020)

Ministerstvo zdravotnictví je v době krizového stavu oprávněno podle § 11 zákona 240/2000 Sbírky:

- zajistit nákup a distribuci potřebných léčivých přípravků, a to i neregistrovaných podle zvláštního právního předpisu; v tomto případě neplatí povinnost oznámení a zveřejnění výjimky podle tohoto zvláštního právního předpisu,

- koordinovat na vyžádání kraje činnost poskytovatelů zdravotnické záchranné služby a poskytovatelů akutní lůžkové péče, kteří mají zřízen urgentní příjem anebo statut specializovaného centra při poskytování neodkladné péče,
- rozhodnout o rozsahu poskytovaných zdravotních služeb poskytovateli akutní lůžkové péče v případě zavádění regulačních opatření podle zákona o hospodářských opatřeních pro krizové stavy.

Součástí krizového plánu je mimo jiné plán nezbytných dodávek zpracovaný podle zákona č. 241/2000 Sb., o hospodářských opatřeních pro krizové stavy a změně některých zákonů, ve znění pozdějších předpisů (MZČR, 2020).

2.4 **Zabezpečovací systém**

Tyto systémy během posledních let prodělaly velký pokrok, a to i díky rozvoji nových technologiií. Jejích cílem je poskytování ochrany konkrétnímu zabezpečenému subjektu, a to souborem technologicko-taktických i organizačních opatření, jejichž cílem je zajištění ochrany. Tento soubor je označován jako zabezpečovací systém. Pro jejich analýzu je potřeba rozlišovat dvě zásadní hlediska:

- operační hledisko
- technické hledisko

Operační hledisko

Operační hledisko se liší v rámci subjektu, pro který je určené. Závisí to na požadovaných specifikách ve způsobu a rozsahu ochrany. S tím je spojena i otázka míry propustnosti zabezpečovacího systému a případný problém eliminace škod v případě, že by došlo k překonání systému. Základní funkční princip IBS se odvíjí od skupiny specifických rysů rizika. Cílená funkce systému je širší a složitější a v otázce bezpečnosti je zapotřebí započítat i možnost dalších faktorů, jako je například požár, výbuch nebo provozní havárie. Fáze operačního hlediska proto zahrnuje i detailní rozbor rizik v objektu a jeho potencionální zranitelnosti. Na základě toho se potom sestaví zabezpečovací systém, v němž jsou operační a technické prvky zkoordinovány pro co nejlepší ochranu objektu. Všechny systémy mají podle organizačního i technického pohledu na problematiku specifickou strukturu, tzv. prvky, které pak nastavují účinnost zabezpečovacích systémů (Uhlář, 2004):

A. Preventivní vliv na potencionálního pachatele

Psychologický, ekonomický nebo společenský vliv na pachatele a schopnost zabezpečovacího systému zamezit ohrožení chráněného zájmu.

B. Detekce

Schopnost systému odhalit jeden nebo více charakteristických znaků ohrožení chráněného zájmu nebo objektu v prostoru, který je kontrolován zabezpečovacími čidly.

C. Diskriminovaná detekce

Je analytický proces, který dokáže částečně rozlišit reálné nebo pouze zdánlivé riziko. Cílem je zaznamenávat každou událost, která by mohla být jen zdánlivě nebezpečná pro chráněný zájem. Efektivnost přímo odpovídá kvalitě zabezpečovacího vybavení.

D. Poplach

Je reakce na pozitivní činnost detekce. Jedná se o blíže nespecifikovanou situaci, která vznikla zasáhnutím do normálního fungování činnosti bezpečnostního systému.

E. Reakce zabezpečovacího systému

Reakce zabezpečovacího systému může mít různé intenzity (od základní mechanické zábrany až po zásah ozbrojených sil). Každopádně, úkolem tohoto prvku je přerušit ohrožení a nebezpečí pro chráněný zájem a učinit to v co nejkratší době. Systém by dále měl být nastaven tak, aby mohl reagovat opakovaně během narušení.

F. Spolehlivost zabezpečovacího systému

Je schopnost zajišťovat požadovanou činnost systému za konkrétních podmínek a po předem nastavenou dobu. Pro tento prvek platí zároveň míra odolnosti jeho samotné zranitelnosti během zajišťování ochrany daného bezpečnostního zájmu. Z toho důvodu se při konstruování těchto zařízení myslí i na průběžné ohlašování funkčnosti jako kontrolu funkčnosti.

G. Efektivnost zabezpečovacího systému

Efektivnost systému můžeme rozdělit na společenskou a ekonomickou. V případě společenské efektivnosti mluvíme o účinnosti boje proti trestné činnosti. Snížení trestné činnosti v dané lokalitě je možné předpokládat po optimálním bezpečnostním nastavení pro rizikové objekty. U ekonomické efektivnosti mluvíme o poměru vlivu systému na eliminaci finančních ztrát v souvislosti s trestnou činností a investovanými prostředky na zabezpečovací

systémy. Jejich efektivnost pak vyjadřuje koeficient ε. Hodnota S udává maximální možné vzniklé škody napadení objektu a také představuje náklady na pořízení bezpečnostního systému. (Uhlář, 2004)

$$\varepsilon = \frac{S}{I} * 100 \qquad [Kč]$$

Technické hledisko

Zásadním rozdílem mezi hlediskem technickým a operačním je fakt, že technické hledisko se v prvé řadě zabývá získáváním informací o situaci chráněného objektu. Tuto funkci zajišťují nejrůznější detektory a čidla, které získanou digitální informaci předávají do informačního nebo řídícího centra. Technická stránka IBS je jedním z hlavních prvků operačního bezpečnostního systému. Jednotlivé prvky, spadající do kategorie technické povahy, jsou obvykle v prvním kontaktu se zdrojem nebezpečí. Každý lidský narušitel může spustit technický zabezpečovací systém, ale je zapotřebí brát v úvahu i výskyt planých poplachů (Uhlář, 2005).

2.5 Fyzická ochrana

Fyzická ochrana je soubor organizačních a také technických prostředků. Jejich hlavním úkolem je zamezení nezákonného jednání s majetkem a zajištění ochrany osob.

Fyzickou ochranu osob a majetku dělíme do tří základních skupin, které jsou:

1. technická ochrana
   - mechanický zábranný systém,
   - poplachový zabezpečovací a tísňový systém,
   - ostatní zabezpečovací systémy.
2. fyzická ostraha
3. režimová ochrana (Brabec, 2001).

Z hlediska prostorového zaměření můžeme fyzickou ochranu rozdělit na pět základních odvětví ochrany:

1) **Obvodová**

Znázorňuje porušení bezpečnosti po obvodu objektu. Tím jsou myšleny i katastrální hranice (vodní toky, zdi, ploty apod.).

2) **Plášťová**

Ohlašuje stav, kdy dojde k vniknutí do pláště objektu porušením některé z mechanických překážek (závory, brány, bezpečnostní dveře atd.).

3) **Prostorová**

Ohlašuje jevy, které nastávají po překonání ochrany plášťové. V situaci, kdy se pachatel nachází uvnitř chráněného objektu, jsou pak využívána čidla, snímače a CCTV kamery pro detekci a monitoring jeho pohybu po objektu.

4) **Předmětová**

Signalizuje bezprostřední kontakt nežádoucí osoby s chráněným zájmem, v tomto případě předmětem. Má za úkol zabránit poškození, zcizení nebo zneužití skupiny předmětů, které se mohou na pracovišti vyskytovat (trezor).

5) **Klíčová**

Zaměřuje se na zabezpečení klíčových míst v objektu. Tedy míst, kde s největší pravděpodobností může dojít k pohybu pachatele a následnému pokusu o narušení bezpečnosti objektu (chodby a schodiště, haly, skladovací prostory). (Uhlář, 2005)

2.6 Technická ochrana

Technická ochrana během posledních let prošla velkým a zároveň rychlým rozmachem. Díky extrémně rychlému rozvoji moderních technologií patří technická ochrana mezi nejhůře překonatelné, a tedy i nejefektivnější. Technická ochrana se neřadí přímo mezi ochranu, ale vytváří na pachatele psychický, konkrétně odstrašující účinek. V obecné rovině se jedná o detekční systém, který získává a přeposílá informaci o narušení stavu v objektu. (Uhlář, 2005)

Tímto narušením rozumíme soubor fyzikálních veličin, které jsou z pohledu zabezpečovacích systémů vyhodnoceny jako subjektivní nebo objektivní zdroj rizika pro objekt chráněného zájmu nebo osob, majetku a informací, kterými zdravotnické zařízení běžně disponuje a využívá pro svůj chod. (Uhlář, 2005)

V celém konceptu bezpečnosti objektu zastává technická ochrana dva základní úkoly. V prvé řadě pracovat s informacemi o pohybu osob a potenciálními protiprávními činnostmi. Ty následně předat pracovníkům fyzické ostrahy pro včasný zásah a eliminaci hrozby nebo alespoň jejích následků. Druhým úkolem je zvyšovat efektivnost fyzické ochrany a tím i snižovat personální, a tedy i finanční náklady na provozování fyzické ostrahy. Toho se docílí nahrazením lidského faktoru technologií, která dokáže plně a někdy i lépe zastoupit pracovníky fyzické ostrahy. (Uhlář, 2005)

2.6.1 Mechanické zábranné systémy

Mechanické zábranné systémy jsou základními pilíři při tvorbě integrovaného bezpečnostního systému. Následně pak z nich vychází podklady pro celý soubor systému bezpečnosti. Jejich funkcí je ztížit nebo přímo zamezit násilnému vniknutí nepovolených osob do chráněné oblasti nebo objektu. MZS zajišťují ochranu skrze svoji vysokou mechanickou pevnost a tím značně prodlužují dobu, po kterou trvá pachateli vniknout do objektu (tzv. minimální doba průlomové odolnosti MZS). Primárním úkolem je tedy vytvořit statickou překážku, která je formulována určitou mírou odolnosti proti destrukčnímu narušení. (Uhlář, 2005)

Minimální dobu průlomové odolnosti stanovujeme nejčastěji pro otvorové výplně (okna, dveře, mříže apod.). Zde platí, že minimální čas, který je zapotřebí pro překonání, tedy min. doba průlomové odolnosti, je zanesen v tabulce č. 1 Bezpečnostní třídy otvorových výplní. (ÚNMZ, 2018)

Proti vloupání do objektu se u mechanických zábranných prostředků dále nastavuje míra odolnosti skrze odporové jednotky (RU), které vycházejí z typových fyzických zkoušek z průlomové odolnosti za použití odstupňované kategorie nástrojů a nářadí. (ÚNMZ, 2018)

Tabulka 1 Rozdělení bezpečnostních tříd podle normy ČSN EN 1627

Bezpečnostní třída	Čas napadení	Použité metody
RC 1	Neuvádí se	Příležitostný zloděj se pokouší o vloupání s použitím malého jednoduchého nářadí a fyzického násilí.
RC 2	3 minuty	Příležitostný zloděj se navíc pokouší o vloupání s použitím jednoduchého nářadí a fyzického násilí. Má malé znalosti o úrovni odolnosti MZS, má málo času a snaží se nezpůsobit hluk.
RC 3	5 minut	Zloděj se pokouší překonat MZS při použití páčidla délky 710 mm a dalšího šroubováku, ručního nářadí, jako malé kladívko, důlčíky a mechanická ruční vrtačka. Zloděj má určité povědomí o systému uzávěru a s tímto nářadím je schopen těchto znalostí využít. Při použití páčidla délky 710 mm lze aplikovat zvýšené fyzické násilí.
RC 4	10 minut	Zkušený zloděj používá navíc zámečnické kladivo, sekeru, dláta, sekáče, přenosnou akumulátorovou vrtačku atd. Toto další nářadí umožňuje zloději rozšířit počet způsobů napadení, případně jejich kombinace – vrtání, sekání, páčení atd. Problém hluku zloděj neřeší.
RC 5	15 minut	Velmi zkušený zloděj používá navíc jednoruční elektrické nářadí, např. úhlovou brusku do průměru kotouče 125 mm, přímočarou pilu atd. Neznepokojuje se hlukem.
RC 6	20 minut	Velmi zkušený zloděj používá navíc dvouruční elektrické nářadí, např. úhlovou brusku do průměru kotouče 230 mm, přímočarou pilu atd. Neznepokojuje se hlukem.

Mechanické zábranné systémy v gesci obvodové ochrany

Stěžejním faktorem pro tuto skupinu technického zabezpečení je jejich prostorová separace od chráněného objektu. V tomto případě se jedná o MZS, které jsou umístěny mimo budovu, respektive na volném prostoru pozemku. Obvykle virtuálně označují hranici pozemku nebo jeho okraj a zároveň vytvářejí pomyslnou právní hranici pozemku. Do těchto bezpečnostních prvků spadají všechny druhy bran, branek, závor, propustí atd., které brání vstupu nepovolených osob na chráněný pozemek. Tyto prvky oplocení pozemku mohou také v závislosti na požadavcích na ochranu úzce spolupracovat různými monitorovacími a detekčními systémy. Současný trh disponuje širokým spektrem produktů s tím největším stupněm zabezpečení (výška oplocení, kvalita a tloušťka materiálu, tvar a velikost ok). (Uhlář, 2004)

Pro sestavení mechanického zabraného systému obvodové ochrany složené z oplocení a pevných bariér lze využít následující materiály:

- Klasické drátěné oplocení – obvykle konstruováno do výšky 1,5 až 2 metry, ze zinkového drátu. Tento druh oplocení je však snadno překonatelný a využívá se k ochraně nejméně významných objektů.
- Bezpečnostní oplocení – zaručuje náročnější kritéria na zabezpečení prostoru. Díky své konstrukci (až 2,5m), použitému materiálu (ocel, beton) a tvaru zajišťuje komplikovanější proniknutí skrz oplocení. Využívají se různé druhy pletiv, bariéry ze žiletkového drátu, palisádové oplocení nebo pevné bariéry.
- Vysoce bezpečnostní oplocení – oplocení konstruované pro nejvyšší ochranu objektů. Díky své až pětimetrové výšce a výplni se využívá pro ochranu průmyslových a vojenských nebo i vězeňských objektů. Patří sem rovný plot a plot se zahnutým koncem na vrcholu a se zaklenutím ze strany od objektu.
- Vrcholové zábrany – doplněk oplocení, který se nachází pouze v kombinaci s oplocením. Slouží jako psychická překážka a sama efektivně zabraňuje pokusu o překonání překážky. Patří sem nástavce z ostnatého nebo žiletkového drátu, pevné nebo otočné hroty či válce.
- Podhrabové překážky – jsou druhem speciálního zabezpečení při stavbě oplocení, u kterého se počítá i s možností, že by mohlo dojít o pokus překonání pod úrovní překážky, tedy podhrabáním terénu a samotné překážky. Používají se ploty doplněné podhrabovými deskami pod povrchem o minimální šířce 1 metr nebo ocelové rošty či ploty s pevnou betonovou podezdívkou.
- Vstupy a vjezdy – ochrana vstupů do objektu je stěžejní pro zajištění bezpečnosti. Zabraňují nekontrolovatelnému pohybu osob a vozidel do objektu a z něj. Ucelená místa kontroly pak výrazně snižují riziko narušení bezpečnosti. Nejjistějším řešením pro eliminaci těchto rizik je zřízení hlídaných bran a branek, umístění závor a turniketů na místa vstupu do objektu. (Uhlář, 2004)

Mechanické zábranné systémy v gesci plášťové ochrany

Pro plášťovou ochranu platí, že jejím hlavním úkolem z hlediska ochrany objektu je co nejvíce zkomplikovat, odradit a v ideálním případě zcela znemožnit přístup nežádoucí osoby přímo do chráněného objektu. K tomu by měl sloužit plášť objektu sestavený z optimálních stavebních prvků samotné budovy a kvalitní a bezpečné otvorové výplně, kterými právě nejčastěji dochází k narušení bezpečnosti. (Uhlář, 2004)

Výše zmíněné stavební prvky budov (stěny, podlahy stropy, střechy apod.) jsou často brány jako automaticky odolné, ale pouze správně zvolená konstrukce a její samotná mechanická odolnost plní pak tu správnou funkci. Mezi krizová místa patří vnější obvodové zdi budov, společné zdi s jinými objekty nebo střechy přízemních objektů. Podle druhu použitého materiálu lze stavby rozdělit na tzv. lehké stavby, jejichž pasivní bezpečnost je minimální a jsou použity matriály jako duté cihly, sádrokarton nebo vlnitý plech. A pak pevné stavební konstrukce, které poskytují odpovídající ochranu s ohledem na tloušťku a kvalitu materiálu. (Uhlář, 2006)

Mnohem rizikovějšími místy v plášti objektu jsou stavební komponenty, bez kterých se většinou neobejdeme, a to jsou dveře, okna, vikýře atd. Na všechny tyto prvky se vztahuje široká škála normovaných parametrů bezpečnosti samotných oken nebo bezpečnostních dveří. Následně se pak dají posílit mřížemi, roletami nebo širokou paletou bezpečnostních skel a fólií. (Uhlář, 2004)

Mechanické zábranné systémy v gesci předmětové ochrany

Pro využití technické ochrany konkrétních předmětů přichází čas tehdy, když nežádoucí osoba úspěšně překonala všechny ostatní prvky zabezpečení. V případě, že je cílem chráněného zájmu nějaký předmět, přichází na řadu jeho uschování do trezorových komplexů. Technická ochrana nabízí klasické trezory, různé varianty bezpečnostních schránek a skříní. Těch je na trhu mnoho druhů s různými stupni odolnosti proti vloupání. (Uhlář, 2004)

2.6.2 Elektronické zabezpečovací systémy

Realizace elektronických zabezpečovacích systémů pro fyzickou ochranu budov řídí norma ČSN EN 20131/Z1. Samotný elektronický zabezpečovací systém (EZS) je poplachový systém, který reaguje na automatickou nebo ruční detekci potencionálního nebezpečí. Identifikuje přítomnost nebezpečí, vstup nebo pokus o vniknutí a narušení bezpečnosti objektu.

EZS je skupina čidel, tísňových hlásičů, prostředků poplachové signalizace, přenosových, zapisovacích a ovládacích zařízení a ústředen, skrze které je pak opticky nebo autisticky signalizováno poplachové hlášení. Výstražný systém lze aktivovat analogovou (např. přerušením drátu) i digitální (detektor pohybu) detekcí. Komunikace mezi jednotlivými detektory narušení a centrální ústřednou může být vedena kabelem, bezdrátově anebo kombinací obou těchto zmíněných způsobů, tj. jeden detektor může být připojen kabelem a druhý bezdrátově. (Křeček, 2008)

V oblasti plášťové ochrany se EZS využívají jako prostředky k dohledu na otevření plášťových výplní nebo jejich destrukci (skla oken nebo dveří). Univerzální variantou pro zabezpečení těchto převážně vstupních prvků jsou díky snadné montáži a vysoké efektivitě magnetické zámky. Pro zajištění okenních výplní se nejčastěji volí ochrana skleněných ploch pomocí tříštivých nebo vibračních čidel, které zaznamenávají vlnění v pevném tělese. Pokud je toto vystaveno poškození, pak tuto informaci o poškození předají jako elektronický signál dál do systému. V posledních letech se objevuje i trend tzv. poplachových fólií, které jsou aplikovány na okenní výplni a uvnitř této fólie jsou vodivé materiály, kdy při jejich přerušení dojde opět k vyslání varovného signálu. (Křeček, 2008)

Pro prostorovou ochranu objektu jsou nejlepší variantou čidla pohybu, která jsou nabízena na trh ve dvou kategoriích. Takzvaná čidla pasivní, která při zjišťování charakteristických rysů napadení pouze zaznamenávají rozdíly fyzikálních veličin ve své blízkosti, a dále čidla aktivní, která vysílají vlastní prostředí a pak reagují na jeho změnu okolními vlivy. Tato čidla mohou pracovat na principu infračerveného, ultrazvukového a mikrovlnného signálu nebo jejich kombinacemi. (Křeček, 2008)

Při nastavování předmětové ochrany lze využít řadu prvků, které byly původně navrženy pro jiné účely. V plném rozsahu lze využít výše zmíněné magnetické zámky, pohybová čidla, infračervené závory nebo různá optická reflexní čidla. Speciálně pro zabezpečení trezorových objektů byla vyvinuta seizmická čidla, která spínají poplach při větších otřesech, způsobených manipulací s bezpečnostní schránkou. (Křeček, 2008)

Poslední skupinou elektronických systémů jsou prvky tísňového hlášení, které se svojí důležitostí v bezpečnostním systému řadí na přední příčky. Jsou využívány k varování a ochraně personálu i veřejnosti v případě bezprostředního ohrožení. Varování může být vyvoláno manuálně nebo zprostředkovaně, například automaticky systémem bez zásahu obsluhy. Je stěžejní, aby tato zařízení byla aplikována na viditelných místech v objektu anebo místě s největším počtem výskytu osob (haly, zasedací místnosti, open office kanceláře,

chodby, schodiště apod.). Tísňové hlásiče jsou obvykle opatřeny krycím sklem, které je při cílené aktivaci nutno porušit. Aktivace tohoto hlásiče pak spustí další sekvence určitého druhu audiovizuálního varování po celé budově. Vybízí tak například k evakuaci nebo spuštění automatického stabilního hasicího systému například v případě požáru. (Křeček, 2008)

2.6.3 Systém kontroly vstupů

Systémy kontroly vstupů jsou využívány převážně tam, kde je potřeba zamezit vstupu nepovolaných osob bez ohledu na předmět chráněného zájmu. Výhodou elektronických systémů vstupu je, že fungují s velkou přesností a mnohem pečlivěji než například fyzická ostraha. Vytlačování lidského faktoru technologiemi je dlouhodobým trendem ve fyzické ochraně, a to nejen z ekonomického hlediska. Velké části vstupních systémů jsou přidělována určitá přístupová práva odvíjející se podle uděleného stupně oprávnění. Systémy pak mohou monitorovat pohyby osob i v konkrétních částech objektu, zamezit přístup do oblastí s vyšším zabezpečením a vyselektovat tak nejvyšší oprávněné osoby. Obvykle je systém automatické identifikace kontroly vstupů koncipován ze šesti základních částí. (Uhlář, 2005)

Identifikační prvek

Tento nosič informací je využíván v nepřeberném množství provedení. Dělí se na čidla kontaktní a bezkontaktní. Dále pak podle tvaru, principu činnosti a z hlediska styku identifikačního prvku se snímacím zařízením. Jako nosič informace může posloužit visačka, přívěšek, identifikační karta, magnetický proužek ale například i podpis, otisk prstu nebo ověření totožnosti hlasem. Prvek zajišťující identifikaci ale musí být adekvátně zvolen podle identifikační technologie a podle podmínek příslušné aplikace. (Uhlář, 2005)

Snímací zařízení

Snímací zařízení je kontaktní hardwarová část, která přijímá do systému informace z osobního identifikačního prvku, převádí data z konkrétního klíče na elektromagnetický signál a ten je poté následně odešle k vyhodnocení do řídící jednotky. Druh snímacího zařízení musí být adekvátní k předem vybranému používanému identifikačnímu prvku v celém systému integrovaného bezpečnostního systému. (Uhlář, 2005)

Řídící jednotka

Tato jednotka je softwarovou částí celého zabezpečovacího vstupního systému. Přijímá elektronické signály od jednotlivých snímačů identifikace a na základě předpřipravených kritérií v interní paměti rozhoduje o vpuštění nebo zablokování hlídaného vstupu pro osobu žádající o vstup do areálu nebo místnosti. Dnešní moderní řídící jednotky disponují plně autonomní schopností rozhodovat na základě vložených dat a stanovisko vyhodnocují okamžitě. Data získaná z jednotlivých identifikačních zařízení zároveň mohou sloužit jako přesná databáze o průchodech osob. Mohou zjistit, kdy a který vstup daná osoba využila nebo se například pouze využít snažila a její přístup byl zamítnut řídící jednotkou. (Uhlář, 2005)

Centrální jednotka

Centrální jednotka koordinuje a sleduje celý proces. Je plně programovatelná a slouží pro kontrolu vstupu do jednotlivých terminálů. Hlavním cílem jednotky je pak sběr důležitých dat, která mají pro kontrolu vstupů nějakou informační hodnotu, jejich vyhodnocení a odpovídající reakce v reálnem čase. Kontrolní software by měl být co nejvíce uživatelsky příznivý, aby nedocházelo k chybovým vyhodnocením přístupového klíče. (Uhlář, 2005)

Blokovací zařízení

Je to část systému, který fyzicky zabrání nebo povolí vstup uvolněním nebo zahrazením vstupního prostoru. V tomto případě se mluví převážně o elektromagnetických zámcích, mechanických závorách nebo turniketech. Tyto prvky vstupních systémů jsou přímo exponovány největšímu náporu síly a jsou nejzatěžovanější součástí celého systému. Pro výběr optimálního blokovacího zařízení je zapotřebí brát zřetel nejen na spolehlivost a funkční vlastnosti, ale i na výběr kvalitních materiálů, správného umístění a odborné montáže. (Uhlář, 2005)

Jednotka zápisu

Je zařízení, které zprostředkovává záznam příslušné informace (jméno, příjmení, osobní číslo, oprávnění, akreditaci a další.) do samotného identifikačního prvku. (Uhlář, 2005)

2.7 Fyzická ostraha

Fyzická ostraha představuje hlídací službu jako součást elementárních činností sboru bezpečnostní služby, která se specializuje na ochranu majetku a osob. Pod pojem hlídací služba spadají nejvíce činnosti požadované zadavatelem, jako je ochrana objektu, jeho zařízení a osob v něm se nacházejících, a také dohlížení na provozní režim v daném objektu. (Černý, 2005)

Fyzická ostraha se přímo podílí na ochraně objektů, osob a majetku skrze předem nastavená preventivní opatření administrativního a výkonného charakteru. Účelem je nejen zajištění bezpečnosti života a zdraví pracovníků, ale i například návštěvníků objektu, a také další chráněné zájmy. Dohlíží na bezporuchový provoz a co nejvíce se snaží předcházet jakékoliv formě kriminální či protiprávní činnosti v souvislosti s bezpečností osob nebo majetku a dohlíží na veřejný pořádek. (Černý, 2005)

V těchto případech pro pracovníky hlídací služby vyvstávají povinnosti:

- zasáhnout při zjištění trestné činnosti nebo jiného protiprávního jednání, avšak adekvátní měrou na chráněný zájem,
- upozornit ostatní složky o poskytnutí pomoci v dané věci přečinu porušení bezpečnosti (Policie ČR, Hasičský záchranný sbor, příp. Zdravotnická záchranná služba),
- obnovit a udržet veřejný klid a pořádek v místě incidentu,
- správně vyhodnocovat situace a adekvátně předcházet konfliktům a dalším nežádoucím událostem (havárie, požár apod.) realizováním příslušných opatření,
- spolupracovat s jednotkami IZS v zabraňování škod na majetku a zdraví v případě nehody. Iniciovat preventivní opatření v oblasti chráněného zájmu v oblasti bezpečnosti a ochrany zdraví.

Při výkonu služby členové fyzické ostrahy zajišťují dohled nad oblastí podle předem nastavených směrnic pro ostrahu. Tím je myšleno zabránění rozkrádání, ztrátě nebo poškození majetku, zabránění neoprávněnému vstupu osob nebo skupině osob do areálu nebo jejich vpuštění bez řádné kontroly, a to jak osobní kontrolou, tak i kontrolou zavazadel nebo vozidel. Během těchto úkonů však nesmí překročit právní rámec daných přepisy, a to hlavně použitím prostředků osobní ochrany a obrany proti napadení, které musí splňovat ustanovení 13 a 14 trestního zákona. (Černý, 2005)

Statická ostraha objektu

Koncept statické ochrany je uplatňován hlavně na pevných stanovištích prvního kontaktu, ze kterých je prováděno střežení pozemku, vstupu nebo budovy. Příslušníci této ostrahy zajišťují takzvanou kontrolně propustkovou službu, při níž monitorují například vstup osob nebo vjezd vozidel a jejich samotné kontroly a zamezují vniknutí neoprávněných osob nebo předmětů do objektu. Dále pak zamezují nekontrolovatelnému vnášení nebo naopak vynášení předmětů nebo materiálu. Podílí se také na plnění povinností v rámci požární bezpečnosti, ochrany bezpečnosti a zdraví a preventivně působí proti vzniku mimořádné události v chráněném objektu. (Černý, 2005)

Pohyblivá ostraha objektů

Cílem zaměstnanců fyzické ostrahy při provádění pohyblivé ostrahy je prostřednictvím systému mobilních hlídek zamezit vniknutí osob nebo vjezdu vozidel mimo kontrolní stanoviště propustkové služby, zabránit naopak vynášení předmětů, materiálu nebo informací z areálu. Zaměstnanci průběžně monitorují celý objekt a pohyb osob v něm a zabraňují podezřelým jedincům v činnosti, která by mohla nějakým způsobem vést k narušení ochrany objektu. (Černý, 2005)

Dále je cílem preventivně působit proti vzniku nežádoucích událostí. Pokud k nim však dojde, tak tito zaměstnanci jako první na místě události provádějí potřebná opatření a poté napomáhají přivolaným jednotkám IZS. Pohyblivá i statická ostraha jsou svými cíli silně provázány. Pro eliminaci hrozeb všech možných příčin je zapotřebí co nejlepší vzájemná spolupráce (Černý, 2005)

2.8 Režimová ochrana

Režimová ochrana je definovaná jako celek všech organizačně administrativních opatření a postupů, které zajištují vyžadovaná kritéria pro funkčnost zabezpečovacích systémů a synchronizaci fungování celého objektu. Dlouhodobě eliminuje zranitelnost objektu před vnějšími škodlivými vlivy, jako jsou drobné krádeže, vandalismus, žhářství nebo získávání citlivých informací. V praxi jsou to především směrnice pro monitoraci pohybu osob po objektu a jejich důvod návštěvy. Pro nastavení kvalitní režimové ochrany a zavedení do praxe je však zapotřebí kvalitní součinnosti všech zaměstnanců organizace a poctivého dodržování nastavených opatření a postupů. (Uhlář, 2004)

Režimová ochrana se rozděluje na vnější a vnitřní. Vnější režimová opatření se zaměřují především na vstup a výstup osob do chráněného objektu. Tím jsou myšleny hlavní a vedlejší vstupy a jejich zabezpečení a případný systém monitorace osob v objektu (např. turnikety nebo identifikační karty), ale i vstupní brány do celého areálu (brány, závory, oplocení apod.) Režimové opatření obecně nastaví kdo, kde a kdy smí nebo nesmí vstoupit nebo opustit objekt či areál organizace chráněného zájmu. Vnitřní opatření jsou pak založena na skupině směrnic upravujících pohyb vozidel a osob po objektu. Režimová ochrana může vymezit určité zóny, pro které je ke vstupu vyžadováno speciální povolení a zpravidla zde bývá zvýšená monitorovací bezpečnost. Dále pak nakládání a transport materiálu, aby byla zajištěna přesná evidence skladovacích prostor a s tím spojená přehledná evidence příjmu a výdeje. V rámci režimových opatření je v případě zdravotnických zařízení potřeba zohlednit i problematiku konfliktů pacient – personál a pacient – pacient. Nastavit co nejefektivnější program předcházení těmto situacím a zároveň adekvátně připravit personál na řešení těchto situací. (Uhlář, 2004)

2.9 Legislativa

Pro odvětví fyzické a technické ochrany není zatím v České republice nastavený konkrétní a ucelený předpis, který by shrnul a jasně definoval problematiku této kapitoly. Proto je zapotřebí všeobecný přehled v níže uvedených zákonech a normách, které vzájemně zastřeší všechny aspekty, parametry a náležitosti, se kterými je možno se setkat při řešení fyzické ochrany.

2.9.1 Nejdůležitější zákony a předpisy

V této kapitole jsou shrnuty všechny zákony a předpisy které určují podobu fyzické ochrany jejího využití a specifikace prostředků a technických prvků v ní využívané.

Zákon č. 1/1993 Sb., Ústava České republiky

Ústavní zákon č. 1/1993 Sb. se řadí mezi dva nejdůležitější zákony české legislativy. Udává základní práva všech občanů České republiky. V tomto zákoně jsou uvedena základní ustanovení zajišťující svrchovanost a jednotnost a zaručující zachování demokratického právního státu. Definuje základní hodnoty a práva. (Zákon č. 2/1993 Sb.)

Dále pak popisuje politický systém, jeho fungování a volbu politických představitelů země. Zákon č. 1/1993 Sb. definuje zákonodárnou moc, moc výkonnou, jakožto vládu, a moc soudní, zastoupenou ústavním soudem. Dále upravuje fungování orgánu Nejvyššího kontrolního úřadu, České národní banky a jednotlivých územních samospráv na úrovni krajů a obcí. (Zákon č. 1/1993 Sb.)

Zákon č. 2/1993 Sb., Listina základních práv a svobod

Zákon č. 2/1993 Sb., základní listina práv a svobod, ve znění starších předpisů, je dalším z dvojice stěžejních právních předpisů pro Českou republiku. Tato listina zastřešuje základní práva a nároky občanů České republiky. Listina je složena z 6 částí neboli hlav a z takzvaných 44 článků. Usnesení č. 2/1993 říká, že lidé jsou si rovni v důstojnosti i právech a jejich práva a svobody jsou nezcizitelné, nepromlčitelné a nezadatelné. Dále pak uvádí postavení státu jakožto subjektu postaveném pouze na demokratických hodnotách, jehož moc může být uplatněna pouze v mezích ustanovených zákonem. (Zákon č. 2/1993 Sb.)

Druhá hlava uvádí konkrétní lidská práva a svobody, hlava třetí pak práva národnostních a etnických menšin. V druhé polovině Listiny jsou pak práva hospodářská, sociální a kulturní, do kterých spadá například právo na svobodnou volbu povolání, spravedlivou odměnu za práci, právo na vzdělání pro každého nebo právo na příznivé životní prostředí. Hlava č. 5 pak definuje právo na soudní a jinou další právní ochranu v rámci státního zřízení. (Zákon č. 2/1993 Sb.)

Zákon č. 372/2011 Sb. o zdravotních službách a podmínkách jejich poskytování

Zákon č. 372/2011 Sb. o zdravotních službách a podmínkách jejich poskytování upravuje zdravotní služby a podmínky jejich poskytování a s tím také spojený výkon státní správy, formy a druhy zdravotní péče, práva a povinnosti všech pacientů a osob pacientům blízkých, poskytovatelů zdravotních služeb, zdravotnických i jiných odborných pracovníků a dalších osob interesovaných v poskytování zdravotních služeb. Dále také podmínky hodnocení kvality a bezpečí zdravotních služeb a činnosti související s poskytováním zdravotních služeb, a zapracovává příslušné předpisy EU. (Zákon č. 372/2011 Sb.)

Zákon o zdravotních sužbách popisuje konkrétní zdravotní služby, pokrývající celé spektrum péče o pacienta. Primárně za účelem předcházení, odhalení a odstranění nemoci, vady nebo zdravotního stavu, dále udržení, obnovení nebo zlepšení zdravotního a funkčního stavu a udržení, resp. prodloužení života a zmírnění utrpení. (Zákon č. 372/2011 Sb.)

U žen pak zajištění pomoci při reprodukci a porodu a lékařské posouzení zdravotního stavu pro všechny pacienty. Pacientem se podle zákona rozumí fyzická osoba, které jsou poskytovány určité druhy zdravotní služby ve zdravotnickém zařízení. (Zákon č. 372/2011 Sb.)

Ošetřujícím zdravotnickým pracovníkem je potom zdravotnický pracovník, který doporučuje, organizuje, provádí a vyhodnocuje individuální léčebný postup u daného pacienta a koordinuje poskytování dalších potřebných zdravotních služeb a informuje rodinné příslušníky. (Zákon č. 372/2011 Sb.)

Vyhláška č. 98/2012 Sb., o zdravotnické dokumentaci

Vyhláška č. 98/2012 Sb., o zdravotnické dokumentaci sumarizuje všechny zákonné podmínky týkající se zdravotnické dokumentace, jež je nedílnou součástí zdravotnického systému. Zaznamenává poskytnutou zdravotnickou péči. Proto jsou zapotřebí jasně stanovená kritéria kdy a v jakých situacích je nastaven rozsah pořizování zdravotnické dokumentace na základě rozsahu poskytovaných zdravotních služeb. Zdravotnická dokumentace vždy obsahuje identifikační údaje poskytovatele péče a údaje pacienta. V návaznosti na diagnostikovaný stav pacienta dokumentace musí obsahovat pracovní závěry a koncovou diagnózu podle Mezinárodní klasifikace nemocí, plán dalšího léčebného postupu a průběžné informace o poskytnutí zdravotní péče, záznam o rozsahu poskytnutých nebo vyžádaných zdravotních služeb a záznam o aktuálním vývoji zdravotního stavu pacienta. (Zákon č. 98/2012 Sb.)

Zdravotnická dokumentace podléhá konkrétním zásadám pro uchování a postupům při jejím vyřazování a zničení po uplynutí doby uchování. Vyřazováním zdravotnické dokumentace je myšleno přezkoumání a organizovaný výběr zdravotnické dokumentace, která již není pro poskytování zdravotních služeb potřebná. Při tomto výběru se rozhoduje o tom, zda zdravotnická dokumentace bude po uplynutí té konkrétní doby uchování vyřazena a navržena ke skartaci. Jednotlivé lhůty uchování se liší podle druhu dokumentu a také podle dalších náležitostí, jako druhu péče nebo pouze jednotlivého zákroku nebo zdravotnického úkonu. Doba archivace se pohybuje u většiny dokumentů v rozmezí 10 až 20 let od vydání dokumentu nebo 10 let po úmrtí pacienta. (Zákon č. 98/2012 Sb.)

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti zákon upravuje konkrétní práva a povinnosti osob a působnost a pravomoc orgánů veřejné moci v oblasti kybernetické bezpečnosti. Dále pak využívá některé konkrétní předpisy Evropské unie, které zajišťují bezpečnost na elektronických komunikačních sítích. Tento zákon se ale nevztahuje na utajované informace v gesci některých informačních zdrojů. Podle tohoto zákona se kybernetickým prostorem rozumí digitální prostředí umožňující vznik, zpracování a výměnu informací. Je tvořené informačními systémy, službami a sítěmi elektronických komunikací. (Zákon č. 181/2014 Sb.)

Dále upravuje v paragrafu 4 bezpečnostní opatření, kterými se rozumí souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru. Orgány a osoby jsou povinny zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury, informačního systému základní služby a významného informačního systému, a vést o nich bezpečnostní dokumentaci. (Zákon č. 181/2014 Sb.)

Zákon č. 40/2009 Sb., trestní zákoník

Zákon č. 40/2009 Sb., Trestní zákoník je složen ze tří hlavních oddílů. První z nich uvádí obecné informace, druhý je zvláštní a třetí pak shrnuje závěrečná ustanovení. V obecném oddílu je shrnuta účinnost trestních zákonů. Je zde popsána problematika trestní odpovědnosti, jednotlivé trestní postihy i okolnosti vylučující protiprávnost. V druhém oddílu je tento zákon zaměřen na konkrétní trestní činy, které mohou být proti ztrátě svobody, životu a zdraví, také trestným jednáním proti osobnímu vlastnictví a lidské důstojnosti. (Zákon č. 40/2009 Sb.)

Okolnosti vylučující protiprávnost jsou takové, které za normálních podmínek splňují podstatu trestného činu, ovšem neberou se za nebezpečné v situaci pro společenství, proto se jako trestný čin neklasifikují. Mezi tyto okolnosti spadá nutná obrana, krajní nouze, oprávněné použití zbraně, svolení poškozeného a přípustné riziko. (Zákon č. 40/2009 Sb.)

- Nutná obrana (§ 29) – je to čin jinak trestný, kterým dotyčný odvrací přímo hrozící, nebo trvající útok na zájem chráněný trestním zákonem.

- Krajní nouze (§ 28) – je čin jinak trestný, kterým dotyčný odvrací nebezpečí přímo hrozící zájmu chráněnému trestním zákonem, ale není trestným činem. Nejde o krajní nouzi v případě, že bylo možno toto nebezpečí za daných okolností odvrátit jiným způsobem.
- Oprávněné použití zbraně (§ 32) – tento paragraf uvádí, že trestný skutek nespáchá ten, kdo užije zbraně v mezích určených jiným právním nařízením.
- Přípustné riziko (§ 31) – trestný skutek nespáchá ta osoba, která v porozumění s dosaženou situací poznání a informacemi, které v rozhodné době o svém dalším opatření měl, vykoná v působnosti svého zaměstnání, funkce nebo postavení společensky prospěšnou událost, navzdory tomu, že by mohl ohrozit nebo porušit zájem chráněný trestním zákonem, nelze-li jinak dosáhnout společensky výhodného výsledku. (Zákon č. 40/2009 Sb.)

Zákon č. 141/1961 Sb., trestní řád

Zákon č. 141/1961 Sb., Trestní řád popisuje práci orgánů, jež působí při objasňování trestných činů a také dopadení pachatelů v rámci trestního řízení. Takto dopadení pachatelé bývají dle zákona řádně potrestáni za své protizákonné jednání. K vymezení osobní svobody osoby ze spáchání trestného činu, těsně po anebo při jeho páchání, může podat kdokoliv. A v případě nutnosti zajištění její totožnosti nebo zjištění konkrétních důkazů existujícího protizákonného skutku. (Zákon č. 141/1961 Sb.)

Vyhláška č. 92/2012 Sb., o požadavcích na technické a věcné vybavení ZZ

Vybavení zdravotnických zařízení jak po stránce technické, tak i materiální upravuje vyhláška č. 92/2012. V ní jsou shrnuty všechny základní prvky vybavení a přístrojů na všech různých typech zdravotnických zařízení a jejich oddělení. (Vyhláška č. 92/2012 Sb.)

2.9.2 Technické normy

Technická norma je technický předpis, který stanovuje zásadní parametry či vlastnosti materiálu, výrobku, součásti nebo pracovního postupu. Technické normy nejsou považovány za obecně závazné, přesto však jsou brány jako kvalifikované předpisy, na které se mohou odkazovat smluvní strany při specifikaci předmětu smlouvy nebo státní orgán v obecně závazných předpisech. Umožňují duplicitu výrobků nebo shodné parametry materiálů pro

výrobu součástek, čímž zlepšují ekonomičnost výroby i zabezpečení výrobků pro jejich používání a odolnost. Využíváním technických norem je pak chráněna i strana spotřebitele. (ÚNMZ, 2020)

Technické normy v České republice nejsou volně šiřitelné a jsou zpoplatněny. Podle rozsahu platnosti se mohou rozdělovat na mezinárodní normy světové (ISO, IEC) nebo evropské (EN), které platí v rámci Evropské unie nebo Evropy.

- Národní normy, jako např. ČSN, DIN, BSI s celorepublikovou účinností, které shrnují široké spektrum problematik. Nižší republikové normy částečně přejímají texty mezinárodních norem. Tyto normy se potom zavádějí do praxe u národních normalizačních sestav jako např. ČSN EN xxxxx, ČSN EN ISO xxxxxx.
- Oborové normy (ON) - tyto byly v ČR zrušeny k 31. 12. 1993 a částečně nahrazeny normami podniku.
- Podnikové normy (PN) - tyto normy si vydávají jednotlivé závody, podniky, skupiny výrobců a společností pro vlastní potřebu a udržení kvality.
- České národní normy ČSN jsou značeny, v případě převzatých mezinárodních (ČSN ISO, ČSN IEC.) a evropských (ČSN EN) norem číslem převzaté normy a třídícím znakem. V případě "čistých" ČSN norem konkrétním třídícím znakem, jenž slouží k přiřazení norem k dané třídě nebo skupině norem. Skládá se z 6 číslic XX YYZZ. XX označujících třídu 01 – 99. Druhé dva znaky YY označují skupinu v rámci třídy. Poslední dvojice čísel ZZ jsou čísla pořadová.

ČSN ISO 31000

Všechny organizace a zařízení jsou vystaveny působení vnitřních a vnějších faktorů, které vytváří ať už přímá nebo nepřímá rizika. Norma ISO 31000 dopodrobna popisuje systematický a logický proces managementu rizik. Zahrnuje samotný proces řízení rizik, poskytuje zásady, rámec a pokyny pro určité situace. Může ji používat jakákoli organizace bez ohledu na její velikost, aktivitu nebo sektor. (ÚNMZ, 2019)

Používání ISO 31000 může organizacím pomoci zvýšit pravděpodobnost dosažení cílů, zlepšit identifikaci příležitostí a hrozeb a efektivně alokovat a využívat zdroje k léčbě rizik. ISO 31000 však nelze použít pro účely certifikace, ale poskytuje vodítko pro programy interního nebo externího auditu. Organizace, které jej používají, mohou porovnávat své

postupy řízení rizik s mezinárodně uznávaným měřítkem a poskytovat spolehlivé zásady pro efektivní řízení, správu a řízení společnosti. (ÚNMZ, 2019)

ČSN P 73 4450-1

Tato norma nastavuje primární požadavky na systémy fyzické ochrany prvku kritické infrastruktury pro maximální omezení dopadu antropogenních hrozeb, včetně teroristického útoku. Tato norma je určena pro všechny objekty kritické infrastruktury, orgány státní správy a samosprávy a poskytovatele bezpečnostních služeb. Pro jiné uživatele může být norma metodickým návodem pro nastavení dostatečné úrovně a rozsahu fyzické ochrany prvků kritické infrastruktury pro daný subjekt. Tato norma je první částí ze souboru norem nastavených pro fyzickou ochranu prvku kritické infrastruktury (ÚNMZ, 2013).

ČSN EN 1627

Tato norma nastavuje podmínky a systém klasifikace vlastností odolnosti proti vloupání do dveří, oken, lehkých obvodových plášťů, okenic a mříží. Zaměřuje se na konkrétní způsoby otevírání: otevírání, sklápění, skládání, otevírání a sklápění, posunování (vodorovné i svislé), navinování, a to i na pevné konstrukce. Dále zastřešuje výrobky jako bezpečnostní kryty dopisních schránek nebo kryty větracích otvorů. Nastavuje požadavky pro míru odolnosti stavebního výrobku proti vloupání. (ÚNMZ, 2012).

Daná norma nezahrnuje odolnost zámků a cylindrických vložek proti napadení paklíči a specifikace pro prefabrikované betonové prvky. Dále se pak norma EN 1627 nezaobírá napadením elektricky, elektronicky a elektromagneticky ovládaných stavebních produktů odolných proti vloupání použitím metody fyzického napadení. (ÚNMZ, 2012)

ČSN EN 50131-1 Všeobecné požadavky

Tato norma má základ v evropské normě EN 50131-1:1997. První část této normy uvádí požadavky pro elektrické zabezpečovací systémy (dále jen EZS), pro užití specifických i nespecifických, pevně zabudovaných propojovacích vedení nebo bezdrátového spojení. Norma však nedefinuje požadavky na EZS pro venkovní aplikace. Dají se však také aplikovat na komponenty EZS nainstalované v budově, kde se normálně instalují na vnější plášť budovy. Norma upřesňuje kritéria provedení nainstalovaných EZS, ale neobsahuje specifikace, návrh, projekce, instalace, provoz a údržbu. Požadavky týkající se EZS spojují sloučené prostředky

detekce, vzájemného propojování, ovládání, komunikace a napájecích zdrojů s dalšími systémy. Provoz daného EZS nesmí být nepříznivě ovlivněn jinými systémy. V normě jsou specifikovány požadavky pro komponenty EZS příslušné klasifikace prostředí. Klasifikace popisuje prostředí, ve kterém je předpoklad největšího využití, a také to že komponent EZS v souladu se svým provedením bude pracovat. (ÚNMZ, 2018)

ČSN EN 50131-2-2 Detektory narušení

Evropská norma popisující požadavky pro pasivní infračervené detektory používané jako prvek poplachových zabezpečovacích systémů instalovaných v objektech. Obsahují čtyři stupně zabezpečení a čtyři různé třídy prostředí. Úkolem detektoru je detekování širokého spektra infračerveného záření vyzařovaného narušitelem. Aby mohl být detektor zapojen do poplachového zabezpečovacího detekčního systému, musí generovat patřičný rozsah signálů nebo zpráv. Tato norma je shrnutím všech kritérií a zkoušek detektorů. (ÚNMZ, 2018)

Některé ostatní druhy detektorů jsou uvedeny v normách řady EN 50131-2. Tato norma také zmiňuje pasivní infračervené detektory namontované v budovách a uvádí stupně zabezpečení od 1 do 4 (dle EN 50131-1) specifických nebo nespecifických metalických nebo bezdrátových detektorů, používaných pro třídy prostředí I až IV (EN 50130-5). (ÚNMZ, 2018)

Detektor musí vyhovovat všem kritériím konkrétního stupně zabezpečení. Funkce, které jsou nadstandardem povinných funkcionalit uvedených v této normě, může detektor obsahovat, ale není přípustné, aby takto ovlivnil dobré fungování těch daných povinných funkcí. (ÚNMZ, 2018)

ČSN EN 50131-2-6 Detektory otevření

Norma EN 50131-2-6 shrnuje kritéria pro detektory otevření (magnetické kontakty), používané jako prvky poplachových zabezpečovacích a tísňových systémů instalovaných v budovách. Jsou určeny pro čtyři stupně zabezpečení a čtyři třídy prostředí. Činností detektoru otevření je rozpoznání změny polohy ovládacího magnetu z předem navolené zavřené pozice, instalovaného na dveřích nebo oknech. Detektor otevření je konstruován ze dvou separovaných částí, které jsou propojeny magnetickým polem. Přerušením spojení mezi těmito dvěma póly je generována zpráva narušení nebo varovný signál. Počet a rozsah těchto signálů nebo zpráv bude širší u systémů vyšších stupňů zabezpečení a záleží na typu nastavení daného systému. Ostatní typy detektorů jsou evidovány v dalších dokumentech uvedených v normách EN 50131 a EN 50131-2. (ÚNMZ, 2018)

ČSN EN 60839-11-1

Tato norma specifikuje minimální funkčnost, požadavky na provozní vlastnosti a metody zkoušení pro elektronické systémy kontroly vstupu a komponenty používané pro fyzický přístup (vstup a odchod) v budovách a jejich okolí a v chráněných prostorách. Neobsahuje požadavky na iniciační zařízení místa přístupu a senzory. Norma nezahrnuje požadavky pro přenos mimo objekty, související s poplachovými a tísňovými systémy. Tato norma se vztahuje na elektronické systémy kontroly vstupu a komponenty určené pro použití v bezpečnostních aplikacích pro zajištění přístupu. Dále obsahuje požadavky na záznam, identifikaci a kontrolu informací. (ÚNMZ, 2014)

ČSN 76 1702

Norma ČSN 76 1702 nastavuje požadavky pro soukromé bezpečnostní služby v oblasti fyzické ostrahy. Tato norma je využívána všemi zprostředkovateli bezpečnostních agentur, organizací nebo jejich poboček zajištujících bezpečnostní služby fyzické ostrahy. Tuto normu může využívat kterýkoliv zadavatel či poskytovatel fyzické ostrahy, který projevuje zájem:

- vytvořit, zavést, udržovat a zlepšovat poskytování fyzické ostrahy podle této normy,
- zajistit shodu s požadavky této normy,
- prokázat takovou shodu ostatním,
- usilovat o certifikaci poskytovaných služeb třetí stranou,
- vyhlašovat, resp. deklarovat shodu poskytovaných služeb s touto normou a požádat o potvrzení tohoto prohlášení třetí stranou. (ÚNMZ, 2014)

ČSN EN 50131-3 Ústředny

Norma udává požadavky, praktická kritéria a zkušební metody pro kontrolu funkcí ústředen poplachových zabezpečovacích a tísňových systémů používaných v budovách, využívajících některá z drátových propojení nebo případně propojení bezdrátové. Je zde popsána skupina požadavků vztahující se i na nápomocná ovládací zařízení aplikovaná uvnitř i venku zajištěných prostorů ve vnitřním a venkovním prostředí. Norma kategorizuje požadavky na realizaci ústředen pro každý ze čtyř stupňů zabezpečení stanovených v evropské normě EN 50131-1 Poplachové systémy - Poplachové zabezpečovací a tísňové systémy -

Systémové požadavky. Požadavky jsou zároveň i odlišné pro všechny čtyři třídy prostředí zahrnující požadavky na vnitřní i venkovní lokaci zařízení. (ÚNMZ, 2010)

ČSN EN 62676-1-1 Systémové požadavky

Norma zahrnuje parametry pro všechny systémy CCTV využívané pro monitorování soukromých i veřejných prostor. Norma nově definuje také čtyři stupně zabezpečení a čtyři třídy vlivu prostředí jako u ostatních dokumentů. Je určena výrobcům a všem dalším organizacím zajišťujícím prosazování práva v dosažení specifikace a přesné specifikace sledovacího systému. V normě nejsou nijak zaneseny požadavky na konkrétní typ technologie, minimální kvalitu a rozlišení obrazu pro konkrétní úlohy sledování. (ÚNMZ, 2014)

ČSN EN1143-1

Tato evropská norma platí pro zkoušení a klasifikaci mobilních skříňových trezorů, vestavěných trezorů do podlahy a stěny, ATM (Automated Teller Machine) trezorů a ATM podstavců, trezorových dveří a komorových komplexů. Norma EN1143-1 je ve zdravotnictví velmi důležitá, ač to tak nevypadá. Přítomnost trezorů je ve zdravotnických zařízeních velmi častá hlavně kvůli úschově opiátů a rizikových léčiv a také pro ukládání důležitých dokumentů nebo cenností pacienta během hospitalizace. (ÚNMZ, 2013)

ČSN EN 356

Norma EN 356 nastavuje požadavky a zkušební procesy pro bezpečnostní zasklení, určené k odvrácení krátkodobého působení síly, což přispívá ke zpoždění vniknutí předmětů anebo osob do chráněného prostoru. V kombinaci s ostatními zabezpečovacími prvky může vniknutí i zcela zabránit. Norma třídí jednotlivé výrobky pro bezpečnostní zasklení do kategorií odolnosti proti působení síly. (ÚNMZ, 2000)

3 CÍLE PRÁCE A VÝZKUMNÉ OTÁZKY

Cíl práce

Stanovit a analyzovat všechny potencionální druhy hrozeb v rámci ochrany zdravotnických zařízení v České republice. Specifikovat fyzickou ochranu pro pacienty a personál zdravotnických zařízení a nastavit minimální průřezové standardy fyzické ochrany.

Výzkumná otázky:

1. Je v dnešní době připravenost zdravotnických zařízení dostatečná?

2. Jaká konkrétní rizika jim hrozí?

4 OPERACIONALIZACE POJMŮ

Definici pojmu ochrana obyvatelstva nejlépe vystihuje celý komplex Koncepce ochrany obyvatelstva do roku 2020 s výhledem do roku 2030 z roku 2013, kterou vydalo ministerstvo vnitra s Generálním ředitelstvím Hasičského záchranného sboru České republiky, která říká že:

Ochrana obyvatelstva je „multiresortní" disciplínou, kterou není možné vysvětlovat a řešit jen jako plnění úkolů civilní ochrany, zejména varování, evakuaci, ukrytí a nouzové přežití obyvatelstva (ve vazbě na Ženevské úmluvy z 12. srpna 1949), ale jako soubor činností a úkolů odpovědných orgánů veřejné správy, právnických a podnikajících fyzických osob a také občanů, které vedou k zabezpečení ochrany života, zdraví, majetku a životního prostředí, v souladu s platnými právními předpisy (MV-GŘ HZS, 2013).

Podle profesora Horáka je ale ochrana obyvatelstva odvozena od pojmu obecné bezpečnosti, která se vztahuje k obecným existenčním hrozbám. Prahem, který definuje bezpečnost, není zajištění blahobytu subjektu, ale jeho samotné přežití, zachování podstatných znaků, životních hodnot a zájmů. Kvalita života je tedy relevantním měřítkem, ovšem za bezpečnostní hrozby jsou považovány ty, které ohrožují existenční podmínky, a právě ty by měly být prioritou v problematice ochrany obyvatelstva (Horák, 2007).

Pojem fyzické ochrany není v současné době nijak konkrétně definován. První definice obecné terminologie přišla od dvou amerických bezpečnostních expertů G. Greena a R. J. Fishera, pracujících v *INTRODUCTION TO SECURITY*, U.S.A.: Security World Publishing Co., Inc. 1993. Podle Greena a Fishera byla fyzická ochrana nastavena pro zabezpečení aktiv různých organizací před nežádoucími vlivy, které by mohly negativně ovlivnit jejich růst, chod a zisk. Do těchto aktiv řadíme v první řadě lidi (zaměstnance, zákazníky), informace a majetek. Hlavní myšlenkou a principem fyzické ochrany je co nejefektivněji ochraňovat osoby a majetek (hmotný a nehmotný) za co nejnižší vynaložené náklady (Fisher, 2008).

Celá koncepce fyzické ochrany některého z objektů nebo přímo organizace bývá obvykle založena na principu tzv. Integrovaného bezpečnostního systému (IBS), což je ucelený soubor bezpečnostních systémů, které jsou vzájemně propojeny a kooperují s okolními faktory, kterým je systém vystaven. (Uhlář, 2005)

IBS je složen ze tří základních pilířů. Prvním z nich je systém mechanické zábrany, který slouží proti narušení nebo napadení objektu jako pevná překážka která brání průniku pachatele do chráněného objektu: to je znázorněno maximálním možným prodloužením počáteční časové prodlevy Δt. Tím je myšlen reálný čas pro překonání překážky mezi časem t_1 (doba napadení objektu) a časem t_2 (doba dokončení napadení objektu). (Uhlář, 2005)

Druhou částí jsou pak signalizační a monitorovací prostředky, které zaznamenávají a sdílí informace o konkrétním napadení chráněného objektu. V lepším případě pak dokážou zajistit bližší určení poškozeného místa a také způsob a dobu, kdy k napadení došlo. Tyto informace pak okamžitě předají do řídícího centra. Posledním je pak systém organizačních opatření a fyzické ostrahy, který následně tyto informace přejímá. Po vyhodnocení nastalé situace přijme adekvátní opatření pro uvedení objektu do definovaného stavu před konkrétním napadením. Nastavení optimální bezpečnosti je závislé na koncepci integrovaného bezpečnostního systému. Ten nabývá maximální účinnosti za předpokladu, že pokryje celý časový interval, který potřebuje pachatel k překonání zábran a vniknutí do objektu nebo spáchání jiné trestné činnosti. (Uhlář, 2005)

Pojem kybernetická bezpečnost, ať už v rovině obecné nebo přímo zaměřené na zdravotnické zařízení, lze vnímat jako odvětví výpočetních technik, tzv. informační bezpečnosti. Cílem informační bezpečnosti je primárně ochrana informací a majetku před zcizením, zničením nebo korupcí Luděk (2017).

Druhou možnou interpretací kybernetické bezpečnosti je definice vycházející ze zákona č 181/2014 Sb. o kybernetické bezpečnosti, který definuje kybernetickou bezpečnost jako *„Souhrn právních, organizačních, technických a vzdělávacích prostředků smiřujících k zajištění kybernetického prostoru“*. (Zákon č. 181/2014 Sb.)

Definici zdravotnického zařízení určuje zákon č. 372/2011 o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách). Podle něj se zdravotnickým zařízením rozumí všechny prostory, kde dochází k poskytování zdravotních služeb a péče. V těchto službách je zahrnuta nedokladná péče, jejímž cílem je omezit nebo zcela zabránit vzniku náhlých stavů, které pacienta bezprostředně ohrožují na životě a v krajním případě by mohly vést až ke smrti.

5 METODIKA

Teoretická část diplomové práce je sepsána na základě tvorby literární rešerše, která byla vytvořena porovnáním dat z odborné literatury a elektronických zdrojů. Mezi hlavní zdroje patřily odborné publikace a články, technická dokumentace a legislativní i technické normy. Z elektronických zdrojů byl nejvíce využíván archív Národní digitální knihovny, který výrazně přispěl při sběru informací vztahujících se k problematice, kterou tato diplomová práce zpracovává. V rámci struktury teoretické části se postupovalo od obecných pojmů, přes popis zdravotnického zařízení, detailní popis segmentu fyzické ochrany a konečně shrnutí základních legislativních a technických norem.

Pro praktickou část diplomové práce byla zvolena metoda analýzy, která měla za cil zjistit odpověď na dvě výzkumné otázky uvedené v kapitole číslo 2. Stanovený postup řešení úkolu zahrnuje jak metodu analýzy, tak i syntézy. Dále zohledňuje poznatky nabité v praktické části této diplomové práce. Otázka zabývající se jaká rizika hrozí zdravotnickým zařízením vycházela z všeobecné Analýzy hrozeb pro českou republiku. Tato analýzy byla zpracována na základě podmětu Koncepce ochrany obyvatelstva do roku 2020 s výhledem do roku 2030, přijaté usnesením Vlády České republiky. Analýzu hrozeb zpracoval odborný team pod záštitou Ministerstva vnitra a byla vybrána jako nejvíce relevantní pro potřeby výzkumu v této diplomové práce. Dokument, který zpracovala pracovní skupina Generálního ředitelství Hasičského záchranného sboru zahrnuje analýzu v širším smyslu, jejíž součástí je identifikace hrozeb, vlastní analýza a následné hodnocení.

Současně je také určena úroveň rizika působení těchto nežádoucích jevů. Výsledky této obecné analýzy byly následně aplikovány přímo na vzorové anonymní zdravotnické zařízení. Všechna rizika byla individuálně posouzena z pohledu primární i sekundárních dopadů na fungování zdravotnického zařízení. Do skupiny primárních rizik byla zařazena ta rizika, která by v případě realizace znamenala celkové vyřazení zdravotnického zařízení z provozu. U sekundárních rizik se pak jedná o situaci, kdy je vyřazena pouze část zdravotnické zařízení, anebo když toto riziko znamená výrazný nárust pacientu na nebo nad hranici kapacity zdravotnického zařízení Tato diplomová práce se nevztahuje na problematiku kybernetických útoků, ale pouze fyzickou ochranu potřebnou pro zajištění fyzické bezpečnosti ve zdravotnických zařízeních.

Pro potřeby druhé výzkumné otázky bylo v první řadě stanoveno vzorové anonymní zdravotnické zařízení. U něj byla provedena podrobná analýza stávajícího stavu fyzické ochrany. Podle zjištěných skutečností byly pak výsledky aplikovány všeobecně na všechna malá a středně velká zdravotnická zařízení. Následně pak byly stanoveny rizikové body zájmu, které byly podrobně rozebrány z pohledu fyzické ochrany. Pro tyto stěžejní body zdravotnických zařízení byly metodou syntézy navrženy zlepšující opatření ve třech hlavních kategoriích fyzické ochrany (mechanické zábranné systémy, elektronické zábranné systémy a fyzická ostraha). V závěru praktické části jsou pak jako výstup práce shrnuta všeobecná doporučení, která by se měla stát alespoň minimálním standardem v oblasti fyzické ochrany všech druhů zdravotnických zařízení.

V kapitole diskuse jsou pak podobně popsány jednotlivé doporučené prvky fyzické ochrany, které by měly být doplněny do bezpečnostního integrovaného systému zdravotnického zařízení, a proč. V závěru diskuse jsou poté rozebrány jednotlivé hrozby, které přímo hrozí zdravotnickým zařízením. Na závěr jsou uvedeny hlavní zlepšovací návrhy, jež by pomohly celoplošně navýšit aktuální úroveň fyzické ochrany všech zdravotnických zařízení.

6 VÝSLEDKY

6.1 Rizika ohrožení zdravotnických zařízení

Následující kapitola uvádí základní seznam rizik, která mohou negativně ovlivnit chod zdravotnických zařízení, ohrozit na zdraví či životě pacienty nebo personál v nich se nacházející. V prvé řadě budou rozebrána rizika vyvstávající ze zdravotnického prostředí a dále pak rizika z prostředí České republiky.

Rizika pro zdravotnická zařízení

Objekt zdravotnického zařízení patří mezi subjekty s možností výskytu obecných bezpečnostních rizik, souvisejících konkrétně s podstatou poskytování zdravotnických služeb a také s variantou, že může dojít k výpadku některého z bezpečnostních systémů. Tato rizika jsou zhodnocena na primární a sekundární dopady a jsou uvedena v tabulce č. 3 níže společně s Analýzou hrozeb pro Českou republiku.

Rizika plynoucí z prostředí

Pro sestavení seznamu hrozeb, jež vyplývají z okolního prostředí, bylo využito dokumentu Analýza hrozeb pro Českou republiku (Paulus, 2015). V tomto dokumentu jsou shromážděna všechna rizika, která mohou na území České republiky nastat. Celkem 72 typů rizik je rozděleno do tří základních skupin.

- Rizika nepřijatelná (riziko nejvyšší priority)
- Rizika podmínečně přijatelná (střední riziko)
- Rizika přijatelná (malé riziko)

Následně je celý seznam hrozeb pro ČR rozčleněn na tyto základní skupiny podle charakteru hrozby: skupinu abiotickou, biotickou, technogenní, sociogenní a ekonomickou.

Rizika podmínečně přijatelná

- N-A-04 sněhová kalamita
- N-A-06 ledovka a náledí
- N-A-07 námraza

- N-A-10 zemětřesení
- N-A-12 svahová nestabilita
- N-A-18 tornádo
- N-A-19 výskyt extrémně nízké teploty
- N-A-20 atmosférické výboje
- N-A-22 dlouhodobá inverzní situace
- N-A-24 požár v přírodě
- A-T-01 únik nebezpečné chemické látky při přepravě
- A-T-07 požár v tunelu
- A-T-08 požár v zástavbě a v průmyslu
- A-T-09 výbuch v zástavbě a v průmyslu
- A-T-10 závažná nehoda v silniční dopravě
- A-T-11 závažná nehoda v letecké dopravě
- A-T-12 závažná nehoda v drážní dopravě
- A-T-15 havárie v metru
- A-T-16 narušení dodávek tepla velkého rozsahu
- A-T-23 narušení funkčnosti poštovních služeb
- A-T-24 propad starých důlních děl
- A-T-29 erupce plynu a vody při poškození sondy na zásobníku plynu a při vrtání na plyn a ropu
- A-T-30 nález nevybuchlé munice
- A-T-31 výbuch ve skladu výbušnin, trhavin, munice, střeliva
- A-S-01 narušení dodávek léčiv a zdravotnického materiálu
- A-S-05 zhroucení sociálního systému

Rizika nepřijatelná

- N-A-01 přirozená povodeň
- N-A-02 přívalová povodeň
- N-A-03 vydatné srážky
- N-A-13 extrémní dlouhodobé sucho
- N-A-17 extrémní vítr
- N-A-21 výskyt extrémně vysoké teploty

- N-B-01 epidemie - hromadné nákazy osob
- N-B-02 epizootie - hromadné nákazy zvířat
- N-B-03 epifytie - hromadné nákazy polních kultur
- A-T-04 únik nebezpečné chemické látky ze stacionárního zařízení
- A-T-06 radiační havárie
- A-T-17 narušení dodávek plynu velkého rozsahu
- A-T-18 narušení dodávek elektrické energie velkého rozsahu
- A-T-19 narušení dodávek ropy a ropných produktů velkého rozsahu
- A-T-20 narušení dodávek pitné vody velkého rozsahu
- A-T-21 narušení bezpečnosti informací kritické informační infrastruktury
- A-T-22 narušení funkčnosti významných systémů elektronických komunikací
- A-T-32 narušení dodávek potravin velkého rozsahu
- A-T-33 zvláštní povodeň
- A-S-02 migrační vlny velkého rozsahu
- A-S-03 narušování zákonnosti velkého rozsahu
- A-E-01 narušení finančního a devizového hospodářství státu velkého rozsahu.

Hodnocení možných dopadů na oblast zdravotnických zařízení

Rizika popsaná v přechozích dvou kapitolách jsou analyzovaná na základě možného negativního dopadu na oblast zdravotnických zařízení:

- Primární dopady – možné fyzické narušení bezpečnosti zdravotnického zařízení (např. úplné vyřazení z provozu nebo přímé ohrožení měkkých cílů).
- Sekundární dopady – potencionální omezení některých stěžejních funkcí nebo událostí vedoucí k přetížení zdravotnických zařízení z důvodu prudkého nárůstu pacientů.

Rizika dle analýzy hrozeb pro Českou republiku

V této části jsou porovnána rizika, která byla vybrána v rámci Analýzy hrozeb pro Českou republiku jako rizika kategoricky podmínečně přijatelná a nepřijatelná. Tato rizika mohou mít přímý či nepřímý dopad na zdravotnická zařízení.

V tabulce č. 2 jsou vyhodnoceny možné primární a sekundární dopady těchto rizik na zdravotnická zařízení. V tabulce jsou zanesena rizika, která mají alespoň jednu pozitivní hodnotu. V analýze rizik pro podmínečně přijatelná rizika jsou zohledněny i situace, které mohou zapříčinit vysokou kumulaci pacientů za krátký čas ve zdravotnickém zařízení a mohou ovlivnit jeho chod.

Tabulka 2: Hodnocení rizik dle Analýzy hrozeb pro Českou republiku

Rizika podmínečně přijatelná		**Primární dopad**	**Sekundární dopad**
N-A-04	sněhová kalamita	Ne	Ano
N-A-06	ledovka a náledí	Ne	Ano
N-A-19	výskyt extrémně nízké teploty	Ne	Ano
A-T-07	požár v tunelu	Ne	Ano
A-T-06	radiační havárie	Ne	Ano
A-T-08	požár v zástavbě a v průmyslu	Ne	Ano
A-T-09	výbuch v zástavbě a v průmyslu	Ne	Ano
A-T-10	závažná nehoda v silniční dopravě	Ne	Ano
A-T-11	závažná nehoda v letecké dopravě	Ne	Ano
A-T-12	závažná nehoda v drážní dopravě	Ne	Ano
A-T-15	havárie v metru	Ne	Ano
A-S-01	narušení dodávek léčiv a zdravotnického materiálu	Ano	Ano
A-S-05	zhroucení sociálního systému	Ano	Ano

Rizika nepřijatelná, plynoucí z prostředí	Primární dopad	Sekundární dopad
N-A-01 přirozená povodeň	Ano	Ano
N-A-02 přívalová povodeň	Ano	Ano
N-A-21 výskyt extrémně vysoké teploty	Ne	Ano
N-B-01 epidemie - hromadné nákazy osob	Ano	Ano
A-T-18 narušení dodávek elektrické energie velkého rozsahu	Ano	Ano
A-T-20 narušení dodávek pitné vody velkého rozsahu	Ano	Ano
A-T-21 narušení bezpečnosti informací kritické informační infrastruktury	Ano	Ano
A-T-22 narušení funkčnosti významných systémů elektronických komunikací	Ne	Ano
A-T-32 narušení dodávek potravin velkého rozsahu	Ano	Ano
A-S-01 narušení dodávek léčiv a zdravotnického materiálu	Ano	Ano
A-S-02 migrační vlny velkého rozsahu	Ne	Ano
A-S-03 narušování zákonnosti velkého rozsahu	Ne	Ano
A-E-01 narušení finančního a devizového hospodářství státu velkého rozsahu	Ne	Ano

Tabulka 3 Rizika pro zdravotnická zařízení

Rizika pro zdravotnická zařízení	Primární dopad	Sekundární dopad
Hrozba umístění nástražného výbušného systému	Ano	Ano
Teroristický útok	Ano	Ano
Vandalismus	Ne	Ano
Napadení ostrahy	Ne	Ano
Selhání ostrahy	Ne	Ano
Napadení skupiny pachatelů	Ano	Ano

Krádež	Ne	Ano
Selhání funkce MZS	Ano	Ano
Selhání funkce EZS	Ano	Ano
Fatální selhání systému rozvodu medicinálních plynů	Ano	Ano
Napadení pacientem	Ne	Ano
Použití biologické, chemické či radiologické látky	Ano	Ano
Únik elektronických dat a kybernetický útok	Ano	Ano
Mimořádná událost způsobená zaměstnancem	Ne	Ano

Dílčí závěr

Tabulky uvedené výše v textu shrnují všechna potencionální rizika hrozící zdravotnickému zařízení. V tabulce 1 a 2 jsou vybrány konkrétní hrozby na základě Analýzy rizik pro Českou republiku. V tabulce 3 jsou poté vydefinovány hrozby a rizika, které jsou přímo specifické pro zdravotnická zařízení.

6.2 Specifikace zdravotnického zařízení

Pro účely této práce bylo zvoleno jedno vzorové zdravotnické zařízení, na kterém bude demonstrována praktická část této diplomové práce. S ohledem na veřejnou diplomovou práci je tato nemocnice bez konkrétního pojmenování. Nemocnice je takto uvedena bez názvu anonymně za účelem ochrany citlivých údajů, které se nachází v diplomové práci a mohly by ji potencionálně poškodit. Obecné závěry, které jsou přijaty v rámci tohoto zařízení, jsou aplikovatelné na všechna malá a středně velká zdravotnická zařízení.

Tato nemocnice je nestátní příspěvkovou organizací. Od 1. 1. 2003 je nemocnice ve vlastnictví a zřizovatelské působnosti kraje. Organizace je zřízena na dobu neurčitou a jejím statutárním orgánem je ředitelka. Nemocnice poskytuje zdravotní péči, ve které je zahrnuta rozsáhlá ambulantní, lůžková, základní specializovaná diagnostická a léčebná péče, nezbytná preventivní péče, lékárenská činnost, dopravní zdravotní služba a lékařská pohotovostní služba.

Oddělení nemocnice

Chirurgické obory:

- Anesteziologicko-resuscitační oddělení a následná intenzívní péče (6 + 8 lůžek)
- Urgentní příjem (5 lůžek)
- Centrální operační sály a sterilizace
- Gynekologicko-porodnické oddělení
- Chirurgické oddělení (83 lůžek + 11 JIP lůžek)
- Ortopedické oddělení (22 lůžek)
- Oční a urologické oddělení (22 lůžek)

Nechirurgické obory:

- Dětské a novorozenecké oddělení (43 lůžek + 3 JIP lůžka)
- Infekční a kožní oddělení
- Interní a neurologické oddělení (88 lůžek + 11 JIP lůžek)
- Oddělení dlouhodobě nemocných a onkologické oddělení (70 lůžek)

Diagnostické obory:

- Oddělení nukleární medicíny
- Oddělení klinických laboratoří a transfúzní služby
- Patologicko-anatomické oddělení
- Radiologické oddělení

Ostatní provozy:

- Dopravní zdravotní služba
- Lékařská knihovna
- Nemocniční lékárna
- Stravovací provoz

Seznam soustavy budov a jejich propojení

V areálu vzorové nemocnice, která byla vybrána pro potřeby této diplomové práce, se nachází celkem 14 pavilonů, které dohromady disponují 16 jednotlivými budovami. Hlavní a největší budova je pavilon chirurgických oborů, který zastřešuje všechna chirurgická oddělení, JIP, ambulance, urgentní příjem, anesteziologicko-resuscitační oddělení, centrální operační sály, sterilizace a také hlavní nemocniční recepci a velký vestibul, kde je možno zakoupit tiskoviny či občerstvení z jídelních automatů. Tato hlavní budova je spojená i systémem výtahu s heliportem, nacházejícím se na střeše hlavní budovy, a s podzemním koridorem, který spojuje pavilon chirurgický s pavilonem interním, ze kterého se dá dále přejít bez nutnosti opustit objekt i na dětské a gynekologicko-porodnické oddělení. Pavilon interní má 3 standardní interní oddělení a jedno neurologické, dále multioborovou jednotku intenzivní péče a v přízemí pak dialyzační středisko, kam dojíždějí pacienti na terapii z celého okresu. Druhá spojovací podzemní chodba vede z chirurgického oddělní k západní straně areálu, kde se nachází oddělení dlouhodobě nemocných, oddělení dlouhodobé intenzivní ošetřovatelské péče a plicní ambulance. Po pravé straně je potom volně stojící budova a v ní je umístěno 2. a 3. oddělení dlouhodobě nemocných. V této části je ještě umístěna budova ředitelství tohoto zdravotnického zařízení.

Ve spodní části areálu se nachází veškeré technické a skladovací zázemí a prostory. Dále se zde nachází hlavní nemocniční lékárna, jsou zde umístěny i garáže a dispečink DZS. Z hlavního pavilonu se dá projít spojovací chodbou do pavilonu RTG a ostatních zobrazovacích metod. V budově tohoto pavilonu se pak ve spodní části nachází celý stravovací provoz, včetně závodní jídelny.

Do celého areálu je vjezd umožněn jednosměrně kvůli omezení dopravních komplikací. Do areálu nemocnice se vjíždí branou horní, která je vestavěna do budovy s biochemickými laboratořemi a druhou tzv. „horní“ lékárnou. Vyjíždí se spodní částí vedle budovy zdravotnické záchranné služby. Obě tyto brány jsou zajištěny závorovým systémem. Oficiální vchody pro pěší jsou určeny též dva. Primární vchod je na hlavní bráně, kde na pohyb osob i vozidel dohlíží ve všední dny od 6 do 15 hodin pověřená osoba na vrátnici. Druhým vstupem je branka bez zabezpečení ze strany do ulic. Tato branka vede k hematologické laboratoři a transfúzní stanici v jedné budově. Celý areál je obehnán železným plotem o výšce 2 metrů. Pod spodní částí areálu jsou dvě parkoviště pro zaměstnance i pacienty. Podél horní části areálu v těsné blízkosti vede jednokolejná železniční trať.

6.3 Stanovení kritických bodů zájmu zdravotnických zařízení v rámci bezpečnosti objektu

Zdravotnické zařízení, jež už bylo popsáno v přechozích částech této práce, je vzhledem k jeho náplni práce rozsáhlý komplex nejrůznějších rizik a hrozeb. V této části diplomové práce budou stanoveny ty stěžejní body zájmu, které by v případě útoku byly pravděpodobně hlavním cílem útočníka.

Analýza pro tuto část diplomové práce bude směřována na vytipované problematické oblasti, které jsou v současné situaci pro zdravotnictví, respektive zdravotnická zařízení potencionálně nejrizikovější. Ty jsou vyjádřeny Vénovým diagramem na obrázku č. 1

Obrázek 1 Body zájmu

Rozbor stěžejních faktorů pro bezpečnost zdravotnického zařízení

Po stanovení základních kritických odvětví lze pro cíle diplomové práce stanovit tři základní body zájmu, které přímo souvisí s civilní ochranou zdravotnického zařízení. Následující seznam tyto prvky řadí se vzestupnou důležitostí (Kalvach, 2016).

1. Měkké cíle v objektu
2. Významnost zdravotnického zařízení v oblasti kritické infrastruktury
3. Citlivé osobní informace pacientů v databázích zdravotnických systémů

Významnost stanovení těchto bodů je stěžejní pro účely této práce. V případě jakéhokoliv útoku na zdravotnické zařízení jsou tyto tři výše zmíněné body nejpravděpodobnějším cílem útočníka, ať už za účelem krádeže citlivých dat, nebo vyřazení systému z jakéhokoliv důvodu. Zájmem útočníka může být i snaha o vyřazení zdravotnického zařízení ze systémů prvků kritické infrastruktury jako nástroj znásobení ničivého účinku útoku například na jeden nebo více jiných prvků, které pak nebude mít kdo ošetřit. V poslední řadě pak přímý útok na pacienty a zaměstnance v měkkém cíli jako manifestace síly či jiného a jakéhokoliv záměru útoku jednotlivce anebo organizované skupiny.

Měkké cíle v objektu zdravotnického zařízení

Obecnou strategii pro ochranu měkkých cílů (soft targets) v České republice vydalo Ministerstvo vnitra ČR v roce 2016 ve formě metodiky, kterou lze aplikovat na široké spektrum situací. Metodika reaguje na zhoršující se bezpečnostní situaci v Evropě a stoupající počet teroristických a extremistických útoků. V minulých letech se zdravotnické zařízení s reálným teroristickým útokem setkalo pouze jednou, a to v prosinci 2019, kdy ve fakultní nemocnici Ostrava aktivní střelec zabil 7 lidí. Více nebezpečných útoků se ale odehrálo v kybernetickém prostředí, ve kterém bylo napadeno několik nemocnic. Některé z nich byly vyřazeny zcela z provozu nebo u nich byla zcizena citlivá osobní data – například kyberútok na počítačovou síť v Psychiatrické nemocnici v Kosmonosech na Mladoboleslavsku. Nejznámějším případem je také celkové odstavení počítačové sítě hackery a následné ochromení nemocnice v Benešově. V pátek 13. března 2020 se terčem útoku stala i Fakultní nemocnice Brno v Bohunicích.

I tento termín fyzické ochrany není zatím přímo definován, ale Metodika Ministerstva vnitra uvádí měkký cíl jako místo s vysokou koncentrací osob a zároveň nízkou úrovní zabezpečení. Díky těmto skutečnostem jsou vybírány jako nejsnadnější cíle s největším rizikem ohrožení zdraví nebo ztráty života. Tím se měkké cíle liší od cílů označovaných jako tzv. hard targets, tedy tvrdých cílů, které na rozdíl od měkkých již disponují některými bezpečnostními prvky (např státní a vojenské objekty, banky apod).

Do kategorie měkkých cílů jsou zařazeny (Kalvach, 2016):

- školská zařízení, koleje, menzy, knihovny,
- církevní památky a místa určená k uctívání,
- nákupní centra, tržiště a obchodní komplexy,
- kina, divadla, koncertní sály, zábavní centra,

- shromáždění, průvody, demonstrace,
- bary, kluby, diskotéky, restaurace a hotely,
- parky a náměstí, turistické památky a zajímavosti, muzea, galerie,
- sportovní haly a stadióny,
- významné dopravní uzly, vlaková a autobusová nádraží, letištní terminály,
- **nemocnice, polikliniky a další zdravotnická zařízení,**
- veřejná shromáždění, průvody, poutě,
- kulturní, sportovní, náboženské a další akce - komunitní centra,

Podle definice uvedené výše byla určena jako kritické oblasti spadající do kategorie měkkých cílů všechna zdravotnická zařízení, poskytující určitý druh léčebné nebo ošetřovatelské péče, a to **fakultní, krajské i okresní nemocnice, polikliniky** a jiná zdravotnická zařízení – všechny typy **specializovaných léčeben, hospiců, domovů pro seniory,** a také například **léčebná lázeňská zařízení.**

Bezpečnostní zajištění měkkých cílů by mělo být vzhledem k jejich charakteristice a uplatnění ve zdravotnictví:

- co nejvíce důsledně účelné kvůli vysokým rizikům, zejména ztrátám životů,
- kreativní kvůli mnohdy omezeným prostředkům, kterými měkké cíle disponují,
- flexibilní kvůli proměnlivosti prostředí, změnám nepřátelských skupin, jejich taktiky útoků a používaným zbraním.

Na základě uvedených kritérii, se z pohledu ohrožení jako nejvíce riziková místa z pohledu ohrožení jeví **ambulantní čekárny** s velkým počtem pacientů na malém prostoru. Hned v zápětí potom **lůžková oddělení jednotek intenzivní péče,** která standardně bývají nedostatečně zabezpečena, a pro případného útočníka by nebyl problém do těchto prostor proniknout. Dalším rizikovým místem jsou **lékárny**. Posledním místem jsou **stravovací prostory,** a to zejména **jídelna** s vysokou koncentrací zaměstnanců, a potom **stánky s občerstvením a bufety.**

Významnost zdravotnického zařízení v oblasti kritické infrastruktury

Systém zdravotnictví je složen ze souboru prvků, mezi nimiž jsou propojeny organizační i materiální vazby. V případě, kdy dojde k přerušení jedné z těchto kritických vazeb, může dojít k ochromení systému. Pokud jde o oblast krizové připravenosti, v oblasti zdravotnických zařízení, je Ministerstvem zdravotnictví stanoveno kritérium (a také krizový zákon) pro poskytování nezbytných služeb. V případě jakéhokoliv narušení kritické infrastruktury jsou aktivovány vytipované prvky, jako konkrétní zdravotnická zařízení, poskytující ambulantní, standardní i intenzivní lůžkovou péči, dále také lékárny, sklady zdravotnického materiálu, výjezdové základny zdravotnické záchranné služby a jejich řídící střediska, která budou nasazena pro záchranné práce a zvládnutí krizové situace.

V případě, že je konkrétní zdravotnické zařízení terčem útoku a je do určité míry vyřazeno z provozu, je pro tyto případy, díky rovnoměrnému rozvrstvení jednotlivých zařízení na území, zajištěno pokrytí lůžkové péče ostatními zdravotnickými zařízeními a redistribuce stávajících pacientů postižené nemocnice, pokud není schopna zajistit standardní úroveň ošetřovatelské péče (Nešporová, Tašlová, 2015).

Dílčím závěrem v hodnocení významnosti zdravotnických zařízení je plná shoda s tvrzením, že zdravotnická zařízení jsou stěžejním prvkem kritické infrastruktury státu a je zcela na místě zajistit těmto složkám maximální možnou ochranu.

Citlivé osobní informace pacientů v databázích zdravotnických systémů

Moderní doba přináší tryskový rozvoj moderních technologií a internet patří mezi ty technologie, na kterých stojí většina celosvětových bezpečnostních systémů. S příchodem internetu stoupla hodnota dat jako komodity tak vysoko, že osobní data pacientů jsou to nejcennější, co zdravotnické zařízení uchovává. Jeho povinností je podle zákona č. 101/2000 Sb. o ochraně osobních údajů chránit tato data nejvyšším stupněm ochrany. V České republice je však dlouhodobě rozpočet na tento segment kybernetické bezpečnosti poddimenzovaný. Není výjimkou, že nemocnice téměř beze změny používají i 10 let a více staré informační systémy.

Podle odborníka na kybernetickou bezpečnost ve zdravotnictví Petra Samka jsou krádeže dat rizikem jak pro zdravotnická zařízení, tak i pro samotné poškozené pacienty. Nemocnice se po krádeži mohou stát obětí vydírání za účelem navrácení informací. V případě pacienta se ale jedná možná i o více zásadní problém. Pokud určitý segment (například banka, pojišťovna) zná podrobnou anamnézu uchazeče, může být tento diskriminován vzhledem ke známým skutečnostem anebo může být peněžní společností zcela odmítnut.

Samek uvádí jako stěžejní krok pro zajištění bezpečnosti informací aktualizovat informační systémy nemocnic. Jako další posun k lepšímu vnímá zavedení elektronických receptů anebo řízené sdílení informací mezi jednotlivými lékaři.

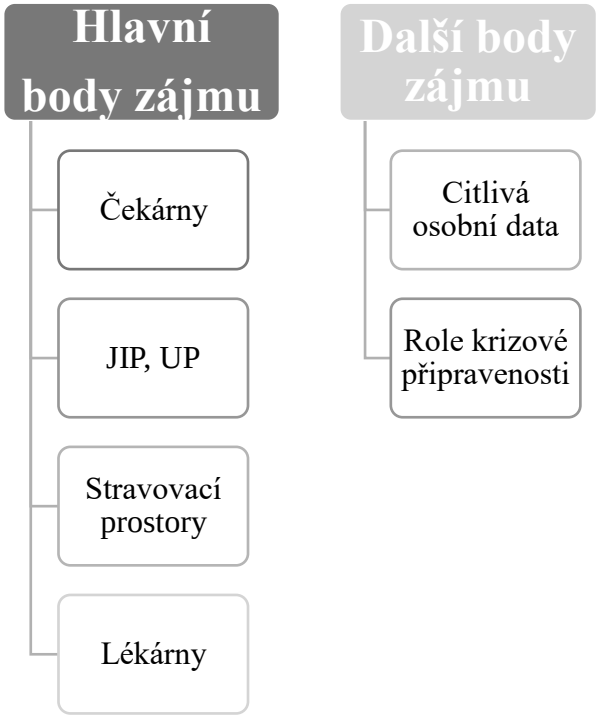
Národní úřad pro kybernetickou bezpečnost uvedl, že se sofistikovanost útočníků zvyšuje, a pro zřizovatele je stále těžší rozpoznat falešné e-maily nebo zprávy na sociálních sítích, které jsou nejčastěji bránou vniknutí útočníka do systému. Tyto podvodné emaily se stávají čím dál věrohodnějšími a aktuálnějšími a často obsahují přílohu se škodlivým kódem či odkaz na nakažené stránky, které stačí navštívit a informační databáze zdravotnických zařízení se dostane pod plnou kontrolu hackerů.

Na základě informací v odstavci sepsaném výše je i citlivost zdravotnických informací pacientů zařazena mezi hlavní body zájmu v rámci analýzy.

Shrnutí zájmový prvků zdravotnického zařízení

Podle textu sepsaného výše lze z pohledu fyzické ochrany u zdravotnických zařízení určit jako zájmové prvky (body zájmu) nebo také tzv. měkké cíle prostory ve zdravotnickém zařízení s nejvyšší koncentrací osob (vše znázorněno na obrázku č. 2). V případě nemocnic a ostatních zdravotnických zařízení se jedná hlavně o ambulantní čekárny a stravovací provozy. Ohledně nedostatečného zabezpečení jsou to i jednotky intenzivní péče.

Další slabou stránkou je riziko ztráty osobních informací pacientů a v neposlední řadě je potencionální hrozbou i vyřazení některého zdravotnického zařízení jako stěžejního prvku kritické infrastruktury. Tato krizová situace může nastat ve chvíli, kdy by došlo k vyřazení zdravotnického zařízení ze systému fyzickým napadením či virtuálním způsobem anebo ochromení infrastruktury výpadkem nezbytných dodávek energií či materiálu.



Obrázek 2 Přehled bodů zájmu

6.4 **Zhodnocení problematiky z pohledu ambulantních čekáren**

Zdravotnické zařízení poskytující ambulantní péče se skládá:

- ze základních prostorů, tj. provozních místností, ve kterých je péče poskytována (ordinace, přípravna nebo místnosti, kde se vykonává základní činnost), a příslušenství pro pacienty
- z vedlejších prostorů, tj. hygienického zařízení pro zaměstnance, úklidové komory a skladu.

Ambulantní čekárna je místnost, která musí být vhodná pro ambulantní pacienty i vozíčkáře. Je určena pro příjem a setrvání pacientů před tím, než navštíví specialistu nebo specializované oddělení. Prostory ambulantní péče musí být podle vyhlášky ministerstva zdravotnictví řešeny takto:

- ordinace je řešena buď jako jedna místnost, tj. společné pracoviště pro lékaře a sestru, nebo jako ordinace lékaře a přípravna, ve které je hlavní pracoviště sestry. Mezi ordinací a přípravnou musí být přímé spojení dveřmi,
- čekárna pacientů musí přímo navazovat na přípravnu nebo ordinaci,

- WC pro pacienty musí mít předsíň vybavenou umývadlem s tekoucí vodou nebo musí být v kabině WC umístěno umyvadlo s tekoucí vodou na mytí rukou. Dveře WC musí být z bezpečnostních důvodů otevíratelné směrem ven,
- čekárna musí mít minimální plochu 7 m^2, pokud není dále uvedeno jinak. Čekárna může být společná pro více ordinací lékařů, pokud má minimální plochu 10 m^2,
- pokud je zdravotní péče (dále jen „péče“) poskytována kojencům, musí mít čekárna minimální plochu 8 m^2 a být vybavena přebalovacím stolem, není-li tento stůl v ordinaci lékaře.

Technické a věcné požadavky na vybavení zdravotnických zařízení ambulantní péče jsou uvedeny v příloze Vyhlášky č. 221/2010 Sb. MZ ČR o technických a věcných požadavcích na vybavení zdravotnických zařízení ve znění pozdějších změn a doplňků.

Ambulantní čekárny byly vyhodnoceny jako riziková místa z pohledu fyzické ochrany ve zdravotnickém zařízení ze dvou zásadních důvodů. V prvé řadě jsou to místa, kde se shlukují velké počty pacientů vyčkávajících na ošetření. To platí pro malé i velké ambulance v nemocnicích, ale i pro čekárny v čistě ambulantních zařízeních, jako jsou polikliniky nebo zdravotnické domy, které jsou organizačně strukturovány na velké množství čekáren, a tudíž jsou místem s vysokým počtem pacientů nacházejících se v uzavřeném prostoru (patro, chodba). Zdravotnická zařízení ambulantní péče musí mít, kvůli zhoršené mobilitě pacientů, řešen přístup do objektů zdravotnických zařízení bezbariérově vodorovnými komunikacemi, rampou nebo výtahem. Standardně v těchto prostorech jsou pacienti vyššího věku anebo je jejich zhoršený zdravotní stav do určité míry limituje. Tento fakt zvyšuje riziko zranitelnosti a staví ambulantní čekárny a pacienty v nich se nacházející do role nejzranitelnějšího cíle pro potencionálního útočníka, který by se rozhodl zaútočit na jednu nebo více čekáren. Zvláštní zřetel je pak zapotřebí brát na čekárnu Urgentního příjmu, která je vystavena nejvíce akutním případům a velkému pohybu nejrůznějších osob.

Dále je potřeba brát velký zřetel na situaci, kdy by bylo zapotřebí urychlené evakuace těchto prostor. Jak už bylo uvedeno výše, otázka evakuace je komplikovaná zhoršeným zdravotním stavem přítomných pacientů a jejich vysokou koncentrací. S ohledem na toto zjištění se pak jako rizikové body pro rychlý odsun osob jeví výtahy k tomu určené – tedy přímo evakuační výtahy stanovené v evakuačním plánu budovy, a úniková schodiště.

Druhým problémem ambulantních i všech ostatních čekáren je jejich 100% otevřenost. Přístup do těchto prostor není téměř v žádných zdravotnických zařízeních nijak kontrolován nebo regulován, a proto je pro potencionálního útočníka zcela bezproblémovou záležitostí provést ať už plánovaný, nebo spontánní útok v reakci na nějakou ze stresových situací. Návrhy na odvrácení nebo částečnou eliminaci rizik popsaných výše se zabývá následující kapitola.

Fyzická ochrana ambulantních čekáren

Tato diplomová práce si dala za cíl stanovit adekvátní fyzickou ochranu kritických bodů zdravotnických zařízení. V případě ambulantních čekáren je náročnost kvalitního zajištění ovlivněna velkou fluktuací osob během krátkého časového období a přísné kontroly by po organizační stránce mohly negativně ovlivnit hlavně z časového hlediska chod celého zařízení. Pro tento bod zájmu jsou stěžejní dostatečná preventivní opatření, která budou mít i psychologický efekt na potencionálního pachatele, a zároveň efektivní systém varování, přivolání represivních složek IZS a případnou evakuaci.

Mechanické zábranné systémy

U ambulantních čekáren nelze přímo efektivně využít mechanických zábranných systému, a to kvůli předpokladu, že do ambulantní péče pacienti sami docházejí, a proto by bylo kontraproduktivní omezit tento princip. V tomto případě může ale částečně pomoci prostorové upořádání, když by došlo ke konstrukčnímu přehrazení například velkých společných čekáren na menší segmenty prostorů pro čekání. Tím jsou myšleny sestavy laviček do boxů případně kójí nebo jiné efektivnější uspořádání.

Elektronické zábranné systémy

Role elektronických zabezpečovacích systémů je ve fyzické ochraně ambulantních čekáren prioritní. V první řadě soustava systémových kamer nabízí dispečerovi v kontrolním středisku dohled nad celým objektem nebo alespoň nad stěžejními místy. Může tedy odhalit podezřelé chování a zabránit kriminální činnosti kontaktováním fyzické ostrahy, která proti pachateli zakročí. Pokrytí kritických bodů je potřeba průběžně aktualizovat a v nejlepším případě by měly záznamy na sebe kontinuálně navazovat. Tak je možné útočníka sledovat celou dobu a mít tak dobrý přehled o jeho poloze pro případný zásah policie anebo alespoň při zpětném vyšetřování či tvorbě případové studie.

Samozřejmostí je pak využití elektronických zámků u nekontrolovaných vstupů do objektu, jako jsou vchody pro personál nebo jiné technické přístupy. U hlavních vchodů je pak možná instalace průchodových rámů s detektory kovů. To lze však pouze v případě, pokud existuje vysoká míra rizika pro konkrétní zdravotnické zařízení, a to například z důvodu lokality nebo politické situace. Tyto kontroly u vstupu však výrazně omezují chod zařízení a jsou kvůli náročnější obsluze nákladnější na personální zajištění. Posledním zabezpečovacím prvkem by mělo být tzv „červené tlačítko“. Toto tlačítko nouzového hlášení je spojeno s řídícím dispečinkem a po jeho stisknutí okamžitě odchází signál o nebezpečí v konkrétním místě jak na dispečink, tak pochůzkové fyzické ostraze. Toto hlášení může být dispečinkem po vyhodnocení následně přeposláno Policii ČR, která na místo vyšle hlídku. Tento prvek by měl být instalován do míst, kde může být snadno aktivován personálem v případě hrozícího nebezpečí.

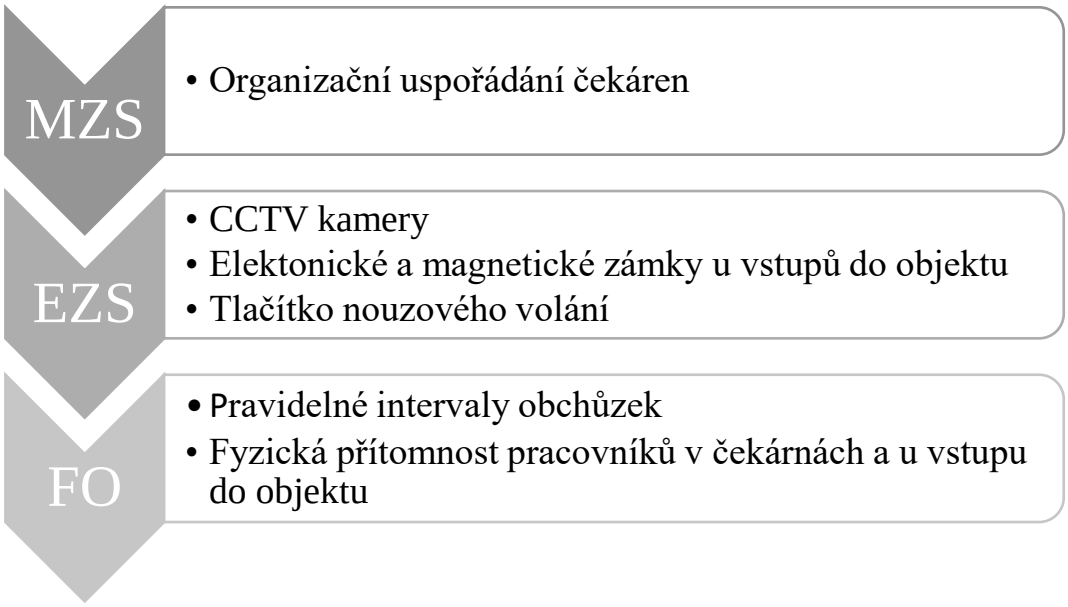
Fyzická ostraha

Fyzická ostraha svojí kompaktností tvoří nejsilnější prostředek pro ochranu ambulantních čekáren. Lidský faktor je u těchto prostor výhodou, jelikož je zapotřebí intuitivního jednání v případě detekce jakéhokoliv problému. Zaměstnanec fyzické ostrahy je schopen na místě řešit individuální problémy, zajistit kontrolu vstupů a také pravidelnou obchůzkovou službou po rizikových místech s vysokým počtem osob eliminuje určité procento nově vzniklých hrozeb. Přítomnost těchto osob v areálu zároveň plní psychologickou prevenci. Mohou se podílet i na organizaci chodu zdravotnického zařízení např. v oblasti dopravní situace nebo jako první zasáhnout na místě vznikajícího konfliktu. Zdravotnické zařízení podle svého uvážení zřídí vlastní dozorovou službu, nebo najme na tento úkol externí bezpečnostní agenturu, která bude na bezpečný chod organizace dohlížet, pokud možno 24 hodin denně. Podle velikosti a počtu ambulancí ve zdravotnickém zařízení je zapotřebí zajistit dostatečný počet proškoleného personálu anebo spolupracovat například s městskou policií po vzoru fakultních nemocnic v krajských městech.

Dílčí závěr

Pro dostatečné zabezpečení ambulantních čekáren je v prvé řadě potřeba myslet na prostorové uspořádání míst k sezení a případně přepažit velkoprostorové otevřené čekárny, a to minimálně optickými překážkami. Jako preventivní opatření pro bezpečí pacientů je potřeba zajistit kamerový dohled nad prostory čekárny, který bude sloužit i pro případnou identifikaci pachatele.

Nejdůležitější roli ale ve fyzické ochraně ambulantních čekáren a osob v nich se nacházejících tvoří pracovníci fyzické ostrahy. Svojí přítomností a svým působením účinně konfliktům předcházejí a měli by být proškoleni i na stejně efektivní řešení. Souhrn těchto opatření je graficky znázorněn v obrázku 3.



Obrázek 3 Zabezpečení ambulantních čekáren

6.5 **Zhodnocení problematiky z pohledu jednotek intenzivní péče**

Jednotky intenzivní péče a také anesteziologicko-resuscitační oddělení, poskytující ošetřovatelskou péči nejzávažnějším pacientům, tvoří společně s urgentním příjmem tři hlavní pilíře péče o pacienty v ohrožení života. V širším pohledu jsou tato tři oddělení i stěžejními pracovišti v zajištění chodu kritické infrastruktury. Mezi obvyklá technická vybavení JIP patří plicní ventilátor, srdeční monitory včetně telemetrie, vnější kardiostimulátory a defibrilátory, dialyzační jednotky, zařízení pro stálé monitorování životních funkcí. Do vybavení se dále řadí široké spektrum přístrojů, jako dávkovací pumpy pro infuze a pro enterální výživu NGS sondou, lineární dávkovače, odsávací pumpy, mobilní RTG a UZ. Dále bývá k dispozici široké spektrum farmakologických prostředků pro léčbu chorobných stavů, pro navození sedace, zajištění analgezie a omezení nozokomiálních nákaz. Jednotek intenzivní péče je v současné době asi 20 druhů. Jde o specializovaná oborová oddělení, která se specializují na odbornou léčbu konkrétních odvětví onemocnění nebo například na věk pacientů.

Jednotky intenzivní péče (JIP, ARO, UP) byly v rámci této diplomové práce zařazeny mezi hlavní body zájmu, které jsou nejvíce rizikové z pohledu ochrany obyvatelstva. Hlavním důvodem, proč jsou tato oddělení zařazena do rozboru, je těžký stav pacientů ležících na těchto odděleních, a fakt, že tito pacienti jsou plně odkázáni na ošetřovatelský personál. V drtivé většině případů jsou životní funkce přímo závislé na přístrojích nebo na lécích, které tyto přístroje dávkují. Zanedbatelným faktorem není ani personální zajištění, které je na jednotkách intenzivní péče výrazně vyšší než na standardním oddělení. To se týká jak lékařů, tak zdravotních sester, ale i pomocného personálu. Nadprůměrný počet personálu v kombinaci s plně imobilními pacienty staví jednotky intenzivní péče do rizikové skupiny, a to hned z několika důvodů. V prvé řadě je JIP měkký cíl, který v případě útoku vystavuje nebezpečí velkou skupinu lidí. Tato oddělení bývají nedostatečně kontrolovaná a zabezpečená, co se týče vstupů, a to pro samotný zdravotnický personál, návštěvy rodinných příslušníku, ale i úplně cizí lidi. Psychicky náročné prostředí pro laickou veřejnost, spolu s negativní informací týkající se zdravotního stavu příbuzného, může opět vyvolat negativní až útočnou reakci. K tomu může dojít přímo i u pacienta, a to z jakékoliv incidence, která může vyústit v násilný konflikt s pacientem. Pro tyto situace by měla být v každém zdravotnickém zařízení zřízena metodika pro řešení těchto situací. Moderní jednotky intenzivní péče jsou projektovány do velkoprostorových místností, kde je uprostřed monitorovací centrála. Pracovní počítače pro personál a lůžka jsou buď umístěny volně v řadě, nebo jsou řešeny boxovým systémem, kde jsou obvykle jedno až dvě lůžka izolovány do proskleného boxu. V případě útoku je tento otevřený prostor nevyhovující. Mezi zvláštní jednotku intenzivní péče patří i urgentní příjem, který svojí funkcí shromažďuje nejrůznější spektrum pacientů, a je tak nejrizikovějším místem, kde může k nějakému útoku ze stran pacientů nebo rodinných příslušníků dojít.

Jednotky intenzivní péče hrají i významnou roli z pohledu kritické infrastruktury. V případě této problematiky je pro zajištění bezpečného chodu zdravotnického zařízení, primárně zajistit i oddělení, které mají právě za úkol zvládnout hlavní nápor pacientů. To mají za úkol dobře nastavená režimová opatření a kvalitní krizové plány. Tyto dokumenty podle aktuální situace nasadí veškeré prostředky, které zajistí, aby byl tento provoz zachován nebo obnoven. V tomto případě je zapotřebí rozlišit, zda je útok mířen přímo na zdravotnické zařízení nebo došlo k vyřazení z provozu až jako sekundární důsledek útoku na jinou část kritické infrastruktury.

Vzhledem k technické náročnosti vybavení a přímé energetické závislosti přístrojů je jednotka intenzivní péče riziková i z pohledu energetického hospodářství. Výpadky energie však jsou ojedinělé, a pokud k nim dojde, jsou zdravotnická zařízení pokrytá stabilní sítí záložních generátorů, které v uzavřeném okruhu okamžitě zajistí dodávku elektrické energie. Náročná je i otázka evakuace, která je v případě jednotek intenzivní péče logisticky nejnáročnější z důvodu přesunu lůžek s přístroji, a dále pak organizace transportu skrze sanitní převozy do jiných, předem domluvených zdravotnických zařízení.

Mechanické zábranné systémy

Využití mechanických zábranných systémů se u fyzické ochrany, aplikované na jednotky intenzivní péče, nedá zcela plně realizovat. Kvalitní bezpečnostní a také protipožární dveře jsou dnes samozřejmostí. Teoreticky se dá využít ochrana předmětová, a tou je myšleno zabránění zneužití zdravotnické materiálu (jehel, nástrojů apod.) pacientem v případě násilného konfliktu s personálem – tedy neponechávat tyto předměty na volně přístupných a viditelných místech.

Elektronické zábranné systémy

Využití elektronických zábranných systémů má stěžejní roli ve fyzické ochraně, která by měla zajistit bezpečnost jednotkám intenzivní péče. V prvé řadě je zapotřebí omezit volný přístup nepovolaným osobám do prostor oddělení. Toho lze nejlépe dosáhnout magnetickým zámkovým systémem dveří, který bude vpouštět pouze ty osoby (zaměstnance), které budou vybaveny speciálním identifikačním zařízením (čipem nebo kartou), skrze něž je mechanismus vpustí dovnitř. Lze využít i číselného zámkového kódu. Řešení skrze identifikační zařízení pro každého zaměstnance při vstupu do areálu nebo na oddělení je výrazně praktičtější i hygieničtější.

Za zvážení stojí i vytvoření dvoufázového vstupu, kdy pro vstup bude zapotřebí projít přes dvojici bezpečnostních dveří. Další prvkem je monitorování prostor vstupů na JIP průmyslovou kamerou, a to jak k celkové monitoraci pohybu osob, tak i kvůli přehledu o personálu. Pokud bude daná osoba žádat o vstup skrze interkom, může na základě podezřelého jednání nebo z jiného důvodu nebýt vpuštěna do prostoru oddělení.

Dále by na jednotkách intenzivní péče nemělo opět chybět tlačítko tísňového volání, které bude umístěno na centrálním pultu pro snadnou aktivaci. Stisk tohoto tlačítka okamžitě uvědomí dispečink a skrze SMS nebo pager zaktivuje i pochůzkovou fyzickou ostrahu, která neprodleně vyrazí na místo problému. Další možností je tísňové volání na linku 158 personálem v případě závažného rizika nebo trestného činu.

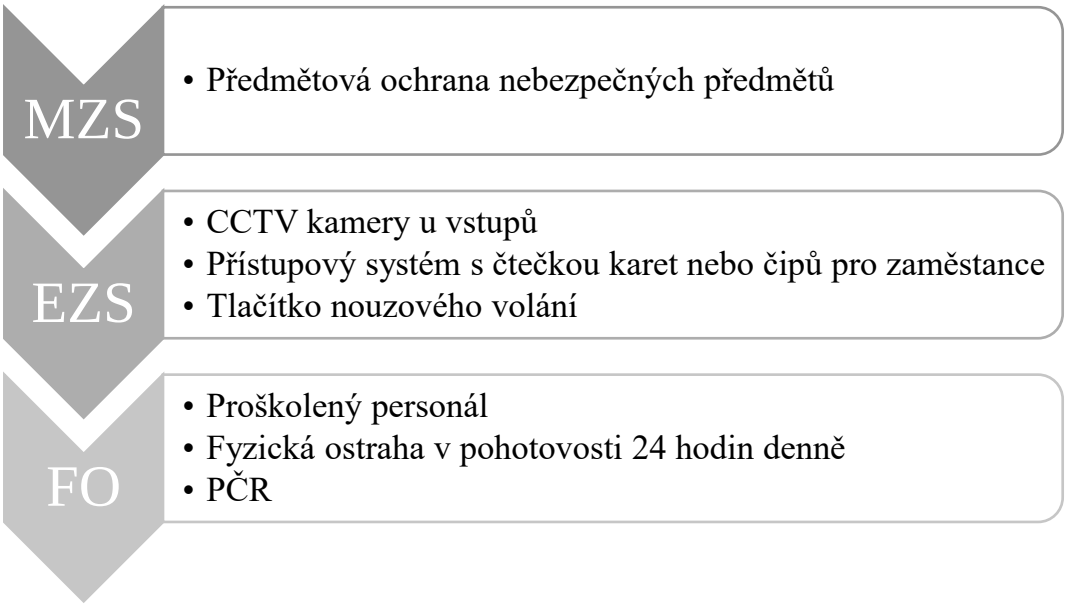
Fyzické ostrahy

Přítomnost fyzické ostrahy na pracovišti v případě ohrožení personálu není vzhledem k nízkému riziku a nízké incidenci efektivní, a tedy i nezbytná. Je ale nutné zajistit, aby byli pracovníci fyzické ostrahy v pohotovosti a v případě nouzového volání například stiskem nouzového tlačítka mobilizováni a schopni se dostavit na místo konfliktu v co nejkratším čase a adekvátně zakročit v rámci svých kompetencí. Pokud bude situace vyžadovat řešení přesahující jejich práva a schopnosti, je zapotřebí kontaktovat linku 158 a přenechat řešení situace Policii České republiky.

V rámci určité formy bezpečnostního školení by mělo dojít k proškolení personálu kvalifikovanou osobou, jak se v těchto situacích zachovat a jak tyto situace řešit. Toto je možno realizovat například formou teambuildingu nebo řešením modelových situací. V gesci personálu je i vpuštění návštěv na oddělení. Vždy by měl dotázaný ohlásit, co je účelem jeho vstupu na oddělení a případně za kterým pacientem jde na návštěvu.

Dílčí závěr

Na rizika hrozící jednotkám intenzivní péče lze nahlížet ze dvou úhlů pohledu. První z nich je napadení zvenku a druhé pak napadení zevnitř. Pokud mluvíme o napadení zevnitř, jedná se o agresi vyvolanou pacientem. Pokud k tomuto dojde, je nutné zamezit zneužití nebezpečných předmětů jako zbraně a mít dostatečně vyškolený personál, který by tuto situaci zvládl, případně by co nejrychleji kontaktoval členy fyzické ostrahy či policii, která tuto situaci dořeší. Odvrácení útoku zvenčí pak zajistí spolehlivý přístupový systém, kde každý zaměstnanec bude mít vlastní identifikační zařízení, kterým se dostane na oddělení. V případě návštěv pacientů na oddělení kontroluje zdravotní sestra podle svého uvážení a skrze kameru příchozí osoby. Navrhovaná opatření jsou graficky znázorněna v obrázku 4.



Obrázek 4 Zabezpečení JIP

6.6 Zhodnocení problematiky z pohledu stravovacích prostorů ve zdravotnickém zařízení

Stravovací prostory ve zdravotnických zařízeních jsou místem, kde dochází k největšímu shlukování osob, a proto byly vyhodnoceny jako rizikové oblasti v případě útoku na měkké cíle ve zdravotnickém zařízení. Každé zdravotnické zařízení ve svých prostorách provozuje nebo pronajímá fyzické osobě určitý druh provozovny, která poskytuje stravovací služby. Jedná se o kavárny, stánky s rychlým občerstvením nebo bufety s širokým spektrem sortimentu, které vyhledávají jak trvale hospitalizovaní nebo pouze ambulantní pacienti, tak i zaměstnanci zdravotnického zařízení. Tyto prostory jsou zcela volně přístupné, stejně jako ambulantní čekárny, a vstup osob sem není nijak výrazně regulován ani kontrolován.

Druhou oblastí je potom prostor stravovacího provozu pro zaměstnance, tedy závodní jídelny, kde dochází k vydávání obědů a v určitou denní dobu je to nejvíce frekventované místo ve zdravotnickém zařízení. Sem docházejí pravidelně téměř všichni zaměstnanci v rámci polední pauzy na oběd. Pokud by došlo k útoku na tyto prostory, bude to s největší pravděpodobností útok mířený a organizovaný za účelem poškození zdraví. Z tohoto důvodu je zapotřebí stanovit adekvátní a účinná opatření, které tomuto riziku maximálně předejdou.

Mechanické zábranné systémy

Mechanické zábranné systémy v ochraně stravovacích provozů ve zdravotnickém zařízení nehrají stěžejní roli. Je však důležité, aby všechny vstupy do těchto provozů byly zajištěny před volným a nekontrolovaným vstupem. Dále je potřeba, aby i tyto prostory byly zabezpečeny kvalitními plášťovými výplněmi, jako jsou okna a bezpečností dveře, které budou následně doplněny elektronickým bezpečnostním systémem. V případě prodejen s občerstvením by bylo zapotřebí pokud možno uzpůsobit prostor pro konzumaci nápojů.

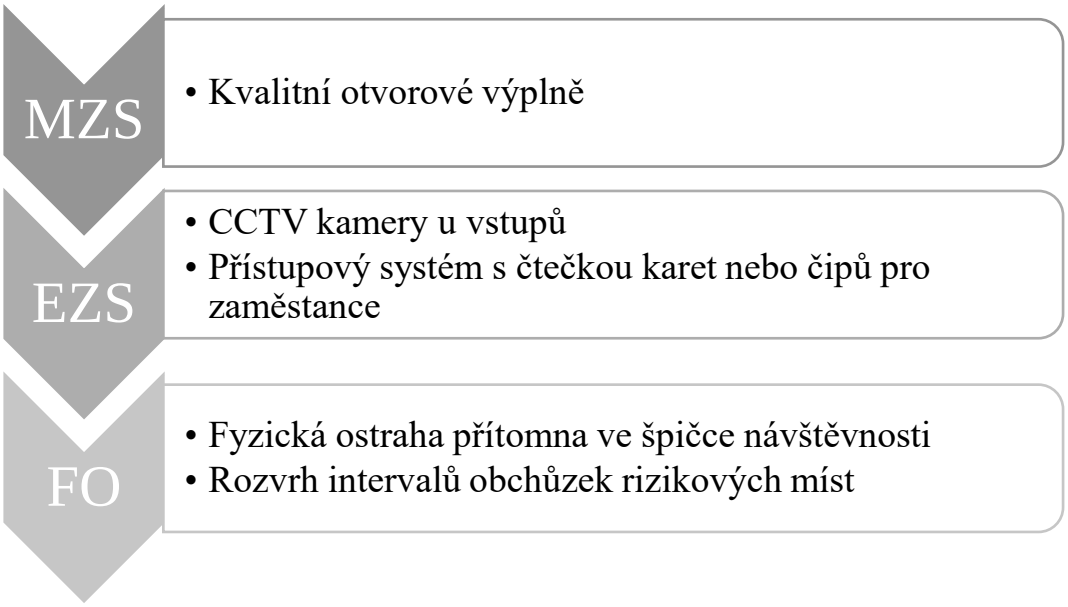
Elektronické zábranné systémy

Uplatnění elektronických zábranných systémů v těchto provozech je omezené. V prostorách určených ke stravování a odpočinku veřejnosti lze pouze umístit kamerový systém. Ten bude skrze řídící středisko monitorovat pohyb osob v těchto částech budovy, a bude vyhodnocovat podezřelé chování nebo kriminální činnost návštěvníků, kterou okamžitě zaznamená a předá k dalšímu řešení pracovníkům fyzické ostrahy nebo uvědomí o tom Policii ČR.

V případě stravovacích provozů, určených výhradně pro zaměstnance, je do zabezpečení možno zahrnout identifikační prvky, které zaměstnanci využívají pro vstupy na svá konkrétní pracoviště. Ty lze centralizovat a využít jako přístupové klíče k přístupovému zařízení, které bude umístěno například u hlavního vchodu do jídelny. Tímto bude zaručeno, že do stravovacího provozu se dostane pouze pověřená osoba, tedy zaměstnanec. Samozřejmostí je umístění jednotky kamerového systému taktéž ke vchodovým dveřím za účelem monitorování pohybu osob.

Fyzická ostraha

Pokrytí stravovacích prostor fyzickou ostrahou je zapotřebí zajistit zejména v hodinách s největší koncentrací osob. Pro provozovny s občerstvením je dobré navrhnout jistý obchůzkový rozpis, kde budou členové ostrahy v pravidelných intervalech dohlížet na předem vytipovaná riziková místa (bufet, kavárna atd.). Pro prostory závodního stravování je doporučeno vyčlenit alespoň jednoho zaměstnance na dozor v časovém období největšího vytížení, tedy kolem poledne, kdy zaměstnanci docházejí na oběd.



Obrázek 5 Zabezpečení stravovacích prostorů

Dílčí závěr

Pro zajištění dostatečné ochrany byla v rámci této diplomové práce stanovena tato opatření: Stěžejní je zajištění přítomnosti vyškolené fyzické ostrahy v období největší vytíženosti. Případně je zapotřebí nastavit intervaly obchůzek, které by eliminovaly riziko vzniku útoku. Důležitým prvkem jsou jako u ostatních bodů zájmu kamerové systémy, které slouží jako prevence a pomohou včasně odhalit potencionální rizika. U zaměstnaneckých prostor vyhrazených ke stravování by bylo vhodné využití přístupového systému do jídelny skrze identifikační zařízení každého zaměstnance.

6.7 Zhodnocení problematiky z pohledu lékáren a ostatních zdravotnických prodejen

Nemocniční lékárny a ostatní prodejny zdravotnického materiálu a pomůcek jsou další položkou na seznamu rizikových bodů z pohledu fyzické ochrany. Problematika tkví ve vysoké fluktuaci osob během celé otvírací doby. Valná většina pacientů ošetřených ve zdravotnickém zařízení si v těchto prostorech vyzvedává prostředky pro další léčení. Nemocniční lékárny jsou také volně přístupné i široké veřejnosti, a tak jsou rizikovým místem v případě útoku na měkké cíle. V těchto případech pak nečekaný útok ozbrojeným útočníkem může skončit velkými ztrátami na životech.

Zajištění těchto prostor bývá komplikované z důvodů volného pohybu osob, které do prostorů těchto prodejen vstupují, a odhalit útočníka je pro IBS nelehkým úkolem.

Mechanické zábranné systémy

Využití mechanických zábranných systémů v případě zabezpečení prodejních prostor není z pohledu bezpečnosti osob příliš efektivní. Zcela jistě je zapotřebí zajistit, aby byly maximálním možným způsobem zajištěny prostory, kde jsou uschovány opiáty a ostatní riziková léčiva. Dále je potřeba zajistit prostory s léčivy, která by mohla být využita pro nelegální výrobu drog nebo prodána na černý trh. Zcizení léků lze předejít instalací kvalitních bezpečnostních dveří a pro uschování těchto léků je zapotřebí zvolit místnost bez oken nebo ty stávající opatřit instalací odolných mříží. V rámci předmětové ochrany je vnitřním nařízením určeno například u opiátů umístění do trezorového systému. Tak je tomu i v případě, že jsou návykové látky přechovávány na odděleních.

Elektronické zábranné systémy

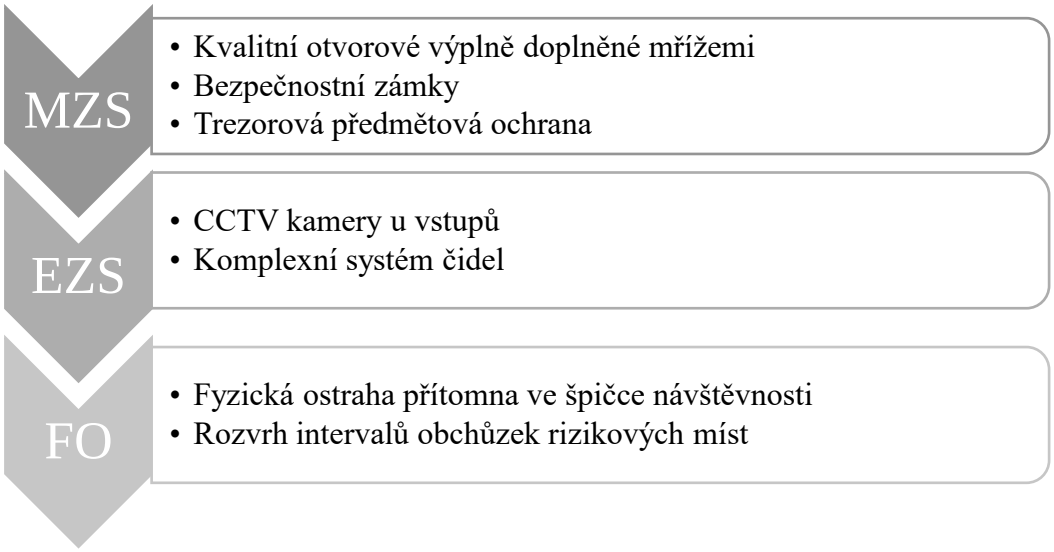
Elektronické bezpečnostní systémy lze využít v případě monitoringu prostor a pohybu osob v něm skrze kamerový systém. Z centrálního dispečinku může pracovník předejít napadení vytipovaných prostor. Dále pak informuje pracovníky daného pracoviště o možné hrozbě a současně mobilizuje zaměstnance fyzické ostrahy. V případě většího rizika kontaktuje i Policii ČR. V ochraně skladovacích prostor lze využít elektronické systémy mnohem efektivněji. Daný prostor může být zabezpečen celou řadou čidel, která jsou napojena na integrovaný bezpečnostní systém, a při jejich spuštění je rozeslána poplašná zpráva na příslušná místa.

Fyzická ostraha

Zajištění dostatečného zabezpečení lékáren v rámci fyzické ostrahy spočívá stejně jako v celém objektu v pravidelných obchůzkách těchto prodejních prostor. Dále může být v období nejvyššího počtu osob v prostorách lékárny trvale přítomen pracovník fyzické ostrahy. Pro dostatečné zajištění tohoto druhu opatření je zcela zásadní sestavit ucelený systém pochůzkové fyzické ostrahy a zahrnout sem prostory lékáren a prodejen se zdravotnickými potřebami.

Dílčí závěr

Z výše uvedeného textu vyplývají jako zásadní bezpečnostní prvky pro ochranu prodejních prostor ve zdravotnickém zařízení především kamerové systémy pro monitoraci pohybu osob. Dalším zásadním bezpečnostním prvkem je zajištění dohledu fyzické ostrahy, která bude sloužit jako preventivní prvek a zároveň složka pro řešení vzniklých problémů. Zajištění bezpečného uložení léčiv se odvíjí od kvalitní plášťové ochrany, dostatečného zabezpečení vstupních prostor a dostatečné úložné trezorové kapacity pro úschovu léků s největším stupněm ochrany. V obrázku 6 jsou tyto navrhovaná opatření graficky shrnuta.



Obrázek 6 Zabezpečení lékáren

6.8 **Zabezpečení areálu zdravotnického zařízení.**

Dostatečné zabezpečení areálu je stěžejním předpokladem pro kvalitní bezpečnostní strategii v ochraně zdravotnického zařízení. V tomto případě jsou prvky fyzické ochrany areálu první překážkou, kterou musí pachatel nebo útočník překonat. Dostatečná ochrana kontroly vstupů do areálu násobí účinnost dalších jednotlivých zabezpečovacích systémů uvnitř budovy. Společně s kamerovým systémem výrazně eliminují riziko vzniku nežádoucí události v otázce bezpečnosti měkkých cílů, nebo například snižují incidenci trestných činů spáchaných na majetku zdravotnického zařízení. Nastavená bezpečnostní opatření by měla efektivně monitorovat pohyb osob po objektu, ale také vjezd do objektu a výjezd vozidel z objektu, který by měl být spojen i s namátkovou kontrolou podezřelých osobních či nákladních aut. Toto prvotní zabezpečení může být v otevřeném prostoru nejefektivnější a je zapotřebí plně využít těchto benefitů ve fyzické ochraně zdravotnického zařízení.

Mechanické zábranné systémy

U zabezpečení objektu je zásadní jak plášťová ochrana, tak i obvodová. V případě obvodové ochrany se jedná o snahu zajistit bezpečnost vyhrazeného území kolem objektu zdravotnického zařízení. Co se týče obvodu, je zapotřebí udržovat kolem celého objektu neporušenou obvodovou zeď budovy z dostatečně odolného materiálu, nebo plot minimálně dva metry vysoký, který zamezí volnému pohybu osob do objektu a následně i ven v případě útěku. V oplocení objektu jsou pak umístěny vstupní prostředky jako brány pro pěší nebo průjezdové brány pro motorová vozidla.

Pro vstup do objektu je zapotřebí určit pouze některé, které budou zabezpečeny zámkovým systémem pro případ uzavření objektu. Vjezdové brány by potom měly mít sofistikovaný systém závorových vjezdů, který bude vytvářet komplexní databázi vozidel. Nejmodernější systémy umí v dnešních dnech zaznamenávat i registrační značku vozidla, která pak může být opět cennou informací při identifikaci pachatele. U vjezdových prostor stojí za zvážení i instalace výsuvných sloupů, které díky svojí konstrukci spolehlivě zastaví i rychle najíždějící vozidlo.

U výplní stavebních otvorů je potřeba dbát na odpovídající normy a v případě nedostačujících zastaralých výplní je na místě zvážit výměnu. Nejdůležitějšími prvky jsou pak dveře, které se skládají ze dvou částí - zárubně a dveřního křídla. Obě tyto části musí disponovat dostatečnou průlomovou odolností.

V případě oken musí být z hlediska bezpečnosti rám okna pevný a dostatečně ukotvený. Volba výplně pak nabízí široký výběr bezpečnostních skel, která se jak v případě oken, tak i dveří dají doplnit kovovou mříží.

Elektronické zábranné systémy

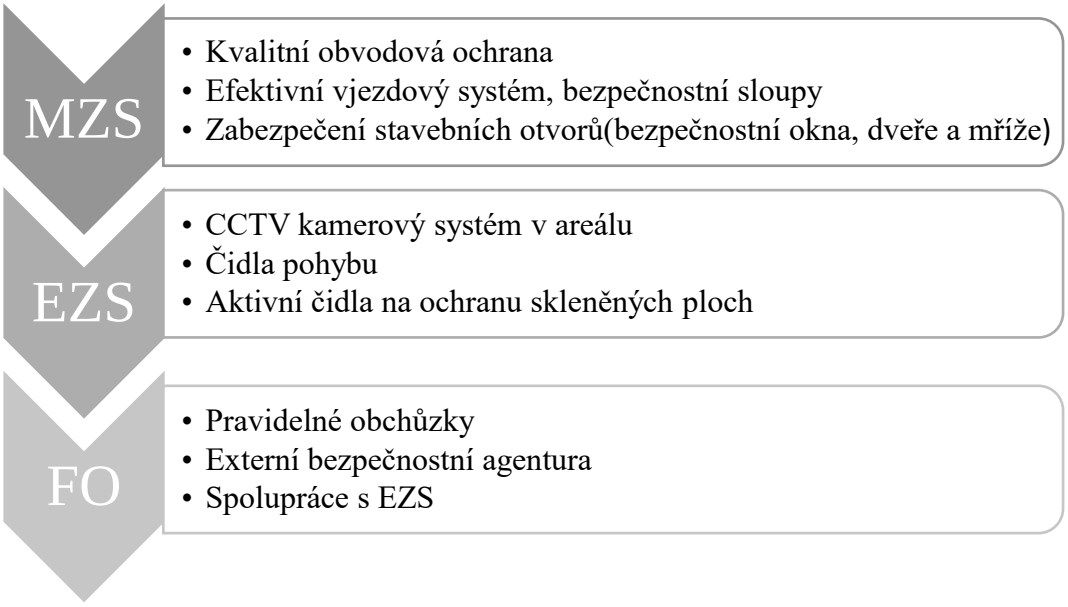
Pokrytí areálu elektronickým zábranným systémem je z hlediska zajištění bezpečnosti nejefektivnějším způsobem. Systematické pokrytí průmyslovými CCTV kamerami na zásadních místech jako jsou vstupy, velká prostranství nebo například místa, kam dojíždí vozidla zdravotnické záchranné služby, předchází a napomáhá odhalení trestného činu. Do méně přehledných nebo tzv. „slepých míst“ lze umístit čidla pohybu, která fungují například na principu infračerveného záření, mikrovln, nebo čidla kombinovaná, která pak potencionálního pachatele odhalí. Všechny přízemní skleněné výplně by měly být doplněny aktivními čidly na ochranu skleněných ploch, které v případě porušení informují centrální dispečink, který vyšle fyzickou ostrahu k dalšímu prošetření a vyhodnocení situace.

Fyzická ostraha

Pro dostatečné pokrytí areálu je zapotřebí vykonávat fyzickou ostrahu za využití uniformovaných či civilně oděných strážců, nebo „na dálku“ pomocí elektronických zabezpečovacích systémů (EZS), případně elektronických požárních systémů (EPS). Tyto dálkové monitorovací systémy jsou přitom obvykle napojeny na pult centrální ochrany (PCO). Tyto pracoviště sbírají, ukládají a vyhodnocují signály ze všech prvků bezpečnostního integrovaného systému. V případě narušení střeženého objektu je okamžitě realizována smluvně stanovená reakce. Tou může být buď zásah jednotky fyzické ochrany, kontaktování policie nebo kontaktování správce atd.

Dílčí závěr

Celkově pro areál zdravotnického zařízení vychází u fyzické ochrany jako stěžejní kvalitní obvodová ochrana, ať už plot nebo obvodová zeď, ale pouze za předpokladu, že splňují dostatečné parametry a zároveň nejsou nikde poškozeny. Využití dalších mechanických zábranných systémů se nachází u otvorových výplní, kde je důležité už během stavby nebo rekonstrukce dbát na stoupající požadavky na bezpečnostní normy a podle nich potom zvolit adekvátní materiál, který zajistí dostatečnou průlomovou odolnost. Co s týče EZS, je to opět komplexní kamerový systém z celého objektu svedený do řídícího centra, které pak mobilizuje pochůzkovou fyzickou ostrahu, která pravidelně provádí obchůzky areálu, kontroluje riziková místa anebo na nich přímo zajišťuje trvalý dohled (viz. obrázek 7).



Obrázek 7 Zabezpečení areálu ZZ

Porovnání zřizovatelů fyzické ostrahy pro zdravotnické zařízení

V případě fyzické ostrahy budov a dalších objektů se využívá pochůzkových strážců, kteří v pravidelných intervalech vykonávají pochůzky po objektu zdravotnického zařízení a zaměřují zvláštní pozornost na předem vytipovaná místa (body zájmu). Ostraha objektů rovněž zahrnuje zajištění pořádku v rámci konání veřejných shromáždění, pomáhání při evakuaci a provádění vyhodnocování bezpečnostních rizik.

Pokud se zdravotnické zařízení rozhodne zřídit vlastní fyzickou ostrahu, získá tím hlavně výhodu komplexnosti a preciznosti bezpečnostní služby. To nastane díky tomu, že bude fyzická ostraha přímo konstruovaná na konkrétní zdravotnické zařízení, a tak snadněji „vychytá“ všechny individuality v koncepci integrovaného bezpečnostního systému. S tím souvisí i lepší znalost zaměstnanců daného objektu, a s tím i spojené intuitivní jednání v daném zdravotnickém zařízení.

Mezi nevýhody vlastní fyzické ostrahy patří prvotní vysoká finanční investice do zřízení této služby. Dále je vedení zdravotnického zařízení zatíženo další administrativou spojenou s rozšířením činností. Posledním problémem může být nedostatek proškoleného personálu nebo komplikace se školením nových zaměstnanců, kteří nemusí dosáhnout takové úrovně jako zaměstnanci externích bezpečnostních firem, které se touto činností dlouhodobě zabývají.

Pokud zdravotnické zařízení osloví externí specializovanou firmu či agenturu, získává tím řadu výhod, které jsou markantní při výběru zřízení této služby. Profesionální firma dokáže plně zajistit vyškolený personál a standardně disponuje i vlastním vybavením. Další výhodou jsou pak bohaté zkušenosti jak agenturních bezpečnostních techniků, tak i samotného personálu. Na druhou stranu využívání služeb externí firmy, která zajišťuje fyzickou ostrahu, bude s největší pravděpodobností finančně náročnější než interní ostraha. Navíc je zapotřebí brát v potaz i nutnost vypsání výběrového řízení pro tuto pozici.

Porovnání současné stavu zabezpečení zdravotnických zařízení

V následující části práce bude zhodnoceno zabezpečení nejmenovaného zdravotnického zařízení, které bylo vybráno jako vzorové pro účely této diplomové práce. Hodnocení aktuálního zabezpečení proběhne z pohledu fyzické ochrany, a to podle zjištěných skutečností v analýze rizikových bodů zájmu sepsaných v předchozích kapitolách. Dále bude vyhodnoceno, zda je toto zabezpečení adekvátní či nikoliv.

Situace v nemocnici, která byla vybrána pro účely diplomové práce, vypadá následovně. Z pohledu obvodové ochrany je celý areál obehnán železným plotem s dostatečnou výškou a odolností. Areál je volně přístupný 24 hodin denně. Pěší mohou pro vstup do areálu zvolit buď hlavní bránu, která je také jako jediná určená pro vjezd motorových vozidel. Dále pak boční branku u hematologické ambulance anebo ze spodní strany areálu přístupovou cestu od parkoviště. Pro vstup do areálu je také možné použít vjezdové prostory. Ty jsou ale primárně určeny pro motorová vozidla a pěší by tuto variantu využívat neměli, protože zde hrozí reálné nebezpečí střetu chodce s vozidlem. Obě tyto brány jsou osazeny závorovým systémem, který vpustí návštěvníky na základě lístkového systému a po zaplacení parkovného je ve spodní části areálu vypustí ven z objektu na hlavní silnici.

Zaměstnanci nemocnice, zdravotnická záchranná služba a některá vozidla zásobování jsou vybavena kartou nebo dálkovým ovládáním pro otevírání těchto bran. Zde se nepředpokládá žádné zneužití vjezdových pravomocí. Během dopoledních hodin je ve všední dny na hlavní bráně přítomen vrátný, který dohlíží na vjezd vozidel. Je-li posuzován kamerový systém v areálu, tak ten se jeví jako nedostatečný. A to z toho důvodu, že pokrývá pouze několik míst a nedává tedy komplexní přehled.

V budovách vzorového zdravotnického zařízení se nachází 4 velké čekárny (chirurgie, interna, UP, RTG nebo ambulancí), kde je během dne vysoká koncentrace osob. Dále asi 10 dalších menších ambulancí nebo pohotovostí, kde je převážně ve všední dny dopoledne zvýšený výskyt pacientů. Všechny tyto prostory jsou volně přístupné a bez zabezpečení některým z prvků integrovaného bezpečnostního systému. Téměř identická situace je v prostorách pro stravování, a to jak v prostorách pro zaměstnance, tak i pro občerstvení pacientů v bufetu, který se nachází hned u hlavní vchodové brány. Zaměstnanecká jídelna v období poledne je nejvíce frekventované místo. V jednu chvíli se zde nachází i s personálem jídelny až 80 lidí.

Vstup do jídelny není nijak zabezpečen, stejně tak jako vstup do dalšího stravovacího provozu. Jediné bezpečnostní pokrytí v těchto prostorech je bezpečnostní kamera, která se nachází ve vestibulu chirurgického pavilonu, kde jsou místa k sezení přibližně pro 30 osob a je zde možnost zakoupit tiskoviny a nápoj z automatu. Tento prostor se využívá pro odpočinek, čekání nebo například pro setkávání návštěv s pacienty.

U všech hodnocených a rizikových bodů zájmu patří jednotky intenzívní péče mezi ty body, které jsou nejvíce zabezpečené. Ve zdravotnickém zařízení, které je bráno jako vzor, se nachází celkem 3 jednotky intenzívní péče. Do této skupiny lze zařadit i prostor urgentního příjmu. Všechny jednotky intenzívní péče mají dva vstupy. Jeden služební pro vstup personálu a příjem pacientů, a druhý civilní pro návštěvy, případně zásobování. Vstup na oddělení je vždy uzamčen cylindrickým zámkem a každý zaměstnanec má od oddělení vlastní klíč. Oba vchody jsou vždy opatřeny zvonkem a interkomem, kterým pak zaměstnanci vpouští pacienta dovnitř. Jiné další zabezpečovací zařízení není v těchto prostorech instalováno. Jediný urgentní příjem má na recepci tlačítko nouzového hlášení, kterým zaktivuje linku 158.

Fyzická ostraha je v případě zkoumaného anonymního zařízení zcela nedostatečná. Fyzickou ostrahu zde zajišťuje externí bezpečnostní agentura. Fyzickou ostrahu pro toto zdravotnické zařízení vykonává každý den od 6 hodin ráno do 14 až 15 hodin odpoledne vždy jeden a ten samý zaměstnanec. Je zřejmé, že sám nemůže dostatečně pokrýt celý areál, ale jeho neefektivní pohyb po areálu spíše evokuje úplnou absenci nějaké formy fyzické ochrany v tomto zdravotnickém zařízení. Je ale samozřejmě zapotřebí brát v potaz finanční prostředky, které vedení nemocnice pravidelně uvolňuje na tyto služby.

7 DISKUSE

Tato diplomová práce si dala za cíl zjistit odpovědi na dvě výzkumné otázky. První z nich, zda je v dnešní době připravenost zdravotnických zařízení dostatečná. V tomto ohledu lze na základě zjištěných skutečností v diplomové práci říct, že připravenost na případně fyzické útoky, tedy dostatečná fyzická ochrana, která by těmto útokům zabránila, dostatečná není. Výzkum realizovaný v této diplomové práci byl proveden na středně velkém vzorovém zdravotnickém zařízení a navrhovaná zlepšení jsou převážně mířena na menší nebo středně velká zdravotnická zařízení.

Na základě výsledků zjištěného stavu zabezpečení zdravotnických zařízení byla navržena následující zlepšení v oblasti zabezpečení celkové fyzické ochrany. V kategorii mechanických zábranných systémů je doporučeno omezení volného průchodu osob do areálu skrze vjezdové brány. A to nejlépe stavební přestavbou těchto prostor nebo zajištěním jejich monitorace. Pokud nejsou tyto prostory využívány celý den, tak je ve večerních a nočních hodinách dočasně uzamknout. Dalším bezpečnostním zlepšením je regulace vjezdu a výjezdu motorových vozidel do areálu zdravotnického zařízení. Toho se docílí umístěním výsuvných sloupů do nájezdových a výjezdových bran. Sloupy v případě potřeby zcela uzavřou celý areál pro motorová vozidla. V otázce plášťové mechanické ochrany je doporučena instalace otřesových čidel do všech skleněných výplní v přízemních patrech budov a jejich napojení na centrální dispečink. Ta pak uvědomí bezpečnostní složky o pokusu násilného vniknutí do objektu.

Ke zvýšení bezpečnostní úrovně zdravotnického zařízení výrazně přispívají i elektronické zábranné systémy. V obecné rovině je základním předpokladem pro zvýšení bezpečnosti rozšíření kamerového systému po celém areálu zdravotnického zařízení a vytvoření centrálního dispečinku, který bude vyhodnocovat informaci mimo jiné i z tohoto kamerového systému. Dalším doporučeným bezpečnostním opatřením je zavedení elektronického centrálního přístupového systému na všechny vstupy na oddělení nebo do ambulancí skrze identifikační kartu nebo čip. S tímto je pak spojeno opatření, které omezuje volný vstup do stravovacích prostor pro zaměstnance, který bude umožněn pracovníkům zdravotnického zařízení právě na základě tohoto identifikačního prvku. Posledním prvkem větší významnosti, který by měl být dodatečně instalován, pokud doteď nebyl, je tlačítko nouzového hlášení. Tím personál v případě nouze neprodleně mobilizuje pracovníky fyzické ostrahy, kteří se v co nejkratší možné době dostaví na místo události. Dále může být signál spojen i s dispečinkem Policie ČR, který automaticky vyšle hlídku k prověření situace.

Třetí hlavní skupinou opatření, která byla hodnocena v této diplomové práci, je fyzická ostraha. V tomto odvětví je pro malá a středně velká zdravotnické zařízení doporučeno přepracovat celou koncepci a organizaci fyzické ostrahy ve zdravotnickém zařízení. Toho lze docílit zejména navýšením počtu zaměstnanců a vytvořením kontrolně pochůzkového harmonogramu s kontrolou kritických míst. Dalším stěžejním krokem pro komplexnost zabezpečení je řízení centrálního dispečinku, který bude shromažďovat informace z poplachových hlásičů a data z kamerového systému, na základě, kterých bude adekvátně reagovat na vzniklé situace. Z tohoto řídícího střediska budou vycházet i konkrétní výzvy, které vyšlou pracovníky ostrahy na konkrétní problematické místo ve zdravotnickém zařízení. Pro fyzickou ochranu zdravotnických zařízení nebyly doposud nastavené žádné standardy, které by stanovily určitou minimální úroveň. Jedním z řešení by byla například konkrétní **metodika ministerstva zdravotnictví,** ve které by byly popsány určité minimální požadavky na fyzickou ochranu, anebo by tato kritéria mohla stanovovat **legislativní úprava.**

Druhou výzkumnou otázkou bylo zjistit, jaká konkrétní rizika obecně hrozí zdravotnickým zařízením. Všechna tato rizika jsou vydefinována v tabulce číslo 3 – rizika pro zdravotnická zařízení. V následující části budou všechna tyto rizika podrobena diskusi.

Vzhledem ke zhoršující se politické i sociální situaci ve světě i Evropě byla do seznamu hrozeb pro zdravotnická zařízení zařazena rizika **teroristického útoku.** S tím je přímo spojené riziko **hrozby umístění nástražného výbušného systému** sloužící jako způsob, kterým teroristické organizace často demonstrují svoji sílu a protlačují svůj záměr. Ačkoliv Česká republika registruje pouze jeden jediný případ teroristické útoku na zdravotnické zařízení, a to útok spáchaný samostatně útočící osobou, a nikoliv organizovanou skupinou, je zapotřebí brát toto riziko v potaz a připravit se na něj. K útoku na zdravotnické zařízení může dojít i v případě, že by útočník nebo skupina útočníků chtěli za účelem demonstrace síly nebo názorového smýšlení způsobit škody na zdraví nebo životě obyvatel. V případě takového útoku může jít i o snahu vyřadit zdravotnické zařízení z řetězce krizové infrastruktury jako další znásobení ztráty na životech v případě útoku na jiný, s největší pravděpodobností měkký, cíl.

Závažnost celé této problematiky ještě násobí riziko v případě, že dojde k útoku **použitím biologické, chemické či radiologické látky.** Biologická válka a bioterorismus je definován jako zneužití mikroorganismů nebo jejich toxinů s cílem poškodit zdraví či způsobit úmrtí lidí, hospodářských zvířat, zničit úrodu a podobně.

Tím narušit nebo znemožnit normální fungování společnosti na napadeném území vyvoláním paniky, spíše než způsobit velké vojenské nebo civilní lidské a materiální ztráty. Biologická agens mohou být zneužita některou z teroristických organizací. V tom případě mluvíme o tzv. bioterorismu. Dochází k užití násilí nebo hrozby násilím s cílem zastrašit protivníka a dosáhnout politických nebo případně politicko-náboženských cílů a jsou využity právě zbraně obsahující biologickou složku. Jako opatření v roce 1972 byla v Moskvě, Londýně a Washingtonu podepsána Úmluva o zákazu vývoje, výroby a hromadění zásob bakteriologických (biologických) a toxinových zbraní a o jejich zničení. V případě využití chemické nebo radiologické látky k útoku je její získání poněkud snazší a samotná likvidace následků útoku nebude tak komplikovanou, i když přesto náročnou operací (Alibek, 2010). Všechny tři typy mohou způsobit škody na zdraví velkého rozsahu. Každá z nich vyžaduje jinou léčebnou strategii, kterou bude zapotřebí poskytnout pacientům, kteří budou po tomto útoku vystaveni působení nebezpečného agens. V případě útoku přímo na nemocnici je stěžejní jakýmkoliv možným způsobem zabránit úniku jakékoli nebezpečné látky.

Další vydefinovanou skupinou rizik je útok na zdravotnické zařízení malou skupinou osob, ale v takovém rozsahu, že se nejedná o teroristický útok. V tomto případě mluvíme hlavně o **vandalismu** nebo **napadení malou skupinou pachatelů či jednotlivcem**. V tomto případě je procentuální šance v našich podmínkách výrazně vyšší a je nespočet případů, které tuto skutečnost dokazují. Lze říct, že v případě vandalismu jsou zdravotnická zařízení výjimečným cílem a toto není problém, který by museli zdravotnická zařízení často řešit. Tento problém se dá vcelku jednoduše pokrýt kvalitním kamerovým systémem nebo případně pochůzkovou službou, která by případná slepá místa areálu hlídala. V případě napadení jednotlivcem nebo skupinou osob je ale zapotřebí v první řadě zvýšit prevenci. Tato hrozba je asi nejvíce zásadní pro zdravotnická zařízení. K těmto situacím dochází i v naší republice, a jak ukázal smutný případ v ostravské nemocnici, tak i jedna osoba může způsobit tragédii. Z toho důvodu je zapotřebí tato problémová místa vyhledávat, vzniku nežádoucí události předcházet a zajistit taková opatření v rámci fyzické ochrany, která tomu zamezí.

Analýza ukázala, že stěžejním prvkem fyzické ochrany zdravotnického zařízení je fyzická ostraha. Jak pochůzková po celém prostoru zdravotnického zařízení, tak statická fyzická ostraha u vjezdů do areálu. Výzkum v diplomové práci také na vzorovém anonymním zařízení ukázal, že fyzická ostraha zdravotnických zařízení je v mnoha případech nedostatečná.

Buď **selháním ostrahy,** ať už z nedostatku personálu, kdy nedokáže dostatečně pokrýt celý areál, nebo selháním profesionálním, kdy smluvní externí agentura nebo samotné vedení zdravotnického zařízení najme nekvalifikované pracovníky. V případě, že dojde k jakémukoliv konfliktu na pozemku zdravotnického zařízení, nastává riziková situace, ve které může dojít k **napadení ostrahy** útočníkem zvenčí, jednak už výše zmíněnou skupinou osob, ale nejčastější útočníci bývají ze strany pacientů. Ať už z řad psychicky nemocných pacientů, pacientů pod vlivem alkoholu, drog, či pouze je to následek stresové situace, ve které se pacient momentálně nachází. I pro tyto situace musí být pracovník fyzické ostrahy připraven reagovat a zároveň je jeho povinností dostavit se na místo konfliktu v nejkratší možné době a pomoci personálu se zvládnutím agresívního pacienta.

Dalším rizikem, definovaným v praktické části diplomové práce, které pomáhá fyzická ostraha eliminovat, jsou **krádeže a ostatní trestné činy,** které se nevyhýbají ani zdravotnickým zařízením. Odcizení majetku může probíhat na pozemku zdravotnického zařízení ale také uvnitř. Tím nejčastěji odcizeným vybavením bývá elektronika. Dochází také k poškození osobních cenností personálu a pacientů. V eliminaci tohoto rizika musí fyzická ostraha úzce spolupracovat s centrálním dispečinkem, který skrze kamerový systém monitoruje situaci po celém objektu, a v tomto případě může buď pachatele zcela zastavit, nebo ho potom prostřednictvím kamerového záznamu dokáže usvědčit.

Jako další riziko byla vyhodnocena situace, kdy z jakékoliv příčiny dojde ve zdravotnickém zařízení k **selhání funkce MZS** a **selhání funkce EZS.** Důvodů, které toto můžou způsobit, je celá řada. Může to být technická závada na systému, například výpadek elektrické energie nebo porucha některého z prvků integrovaného bezpečnostního systému, který pak navazuje na řetězec dalších opatření, a tím pak může dojít k disfunkci celého systému. Samozřejmě může dojít k cílenému narušení systému pachatelem nebo skupinou pachatelů, kteří potřebují vyřadit tyto systémy z provozu v případě, že chtějí narušit bezpečnost a určitým způsobem ohrozit zdravotnické zařízení, pacienty nebo zdravotnický personál.

Poslední skupinou rizik jsou nebezpečí, která přímo souvisí s ošetřovatelskou péčí, která je poskytována ve zdravotnických zařízeních. Na základě rozboru rizik bylo určeno riziko, kdy by došlo k **fatálnímu selhání systému rozvodu medicinálních plynů**. K této závažné komplikaci může dojít jak technickou závadou, tak se může systém rozvodů medicinálních plynů stát cílem útoku za účelem vyřadit zdravotnické zařízení z provozu. Tím pak nepřímo zaútočit na tu skupinu pacientů, kteří jsou v tu chvíli odkázáni na oxygenoterapii nebo umělou plicní ventilaci.

I pro tyto případy je zapotřebí dostatečně zabezpečit centrální rozvod mechanickými i elektronickými zábrannými systémy, ale také mít uskladněnou dostatečnou zásobu kyslíku v tlakových lahvích jak na odděleních, tak i v centrálním skladu zdravotnického materiálu.

Dále může být chod zdravotnického zařízení ohrožen **mimořádnou událostí způsobenou zaměstnancem.** Druhů mimořádných událostí je celá řada. V případě tohoto rizika se ale nedá předpokládat žádný primární dopad na chod nemocnice, ale pouze sekundární následky, a to pouze u těch nejzávažnějších případů. Posledním velkým rizikem se stoupající závažností je **únik elektronických dat a kybernetický útok.** Tato problematika však nespadá do gesce fyzické ochrany, a proto nebyla v rámci této diplomové práce řešena.

8 ZÁVĚR

Předložená diplomová práce je zaměřena na posouzení míry zabezpečení zdravotnických zařízení z pohledu fyzické ochrany. Toto téma bylo zvoleno na základě aktuálnosti tohoto tématu ve společnosti. S ohledem na stoupající tendenci útoků na zdravotnická zařízení si práce dala za cíl zhodnotit míru fyzické ochrany zdravotnických zařízení a dále pak stanovit potencionální rizika, která zdravotnickým zařízením v současné době hrozí.

V teoretické části diplomové práce je přehledně zpracována problematika fyzické ochrany. Jednotlivé druhy, možnosti využití a také konkrétní prvky, které jsou k zabezpečení daných sektorů využívány. V závěru první části je připojena zpracovaná základní legislativa a souhrn nejdůležitějších technických norem, které jsou stěžejní pro nastavení správné koncepce fyzické ochrany zdravotnického zařízení.

Pro potřeby výzkumu praktické části této diplomové práce byla zvolena hodnotící analýza. Pro účely první výzkumné otázky bylo vybráno vzorové anonymní zdravotnické zařízení. Po zhodnocení aktuálního stavu tohoto zařízení byl vyhodnocen celkový závěr odpovídající všem malým a středně velkým zdravotnickým zařízením. Výzkum potvrdil předpokládaný výsledek. Fyzická ochrana byla ve všech ohledech shledána jako nedostatečná, a proto byla následně navržena zlepšující opatření. Analýza ukázala, že stěžejním prvkem fyzické ochrany zdravotnického zařízení je fyzická ostraha. A to jak statická fyzická ostraha u vjezdů do areálu, tak i pochůzková služba po celém prostoru zdravotnického zařízení.

Výzkum v diplomové práci také na vzorovém anonymním zařízení ukázal, že fyzická ostraha zdravotnických zařízení je v mnoha případech nedostatečná. Výstupem této části práce je doporučení ke zpracování konkrétní metodiky, která by nastavila minimální pravidla pro fyzickou ochranu zdravotnických zařízení. Dalším doporučením nápravy je legislativní úprava ze strany Ministerstva zdravotnictví.

Druhá výzkumná otázka si kladla za cíl zhodnotit rizika, která v současné době hrozí zdravotnickým zařízením. Výsledek těchto rizik je přehledně zpracován do tabulek na začátku praktické části. Tato rizika vycházejí z Analýzy hrozeb pro Českou republiku, která byla pro účely diplomové práce aplikována na zdravotnická zařízení.

Pro potřeby diplomové práce byla využita metoda analýzy, jejíž výsledky jsou zpracovány v praktické části zabývající se riziky pro zdravotnická zařízení, zhodnocením zabezpečení a s tím spojeným návrhem na zlepšení současné situace.

V této diplomové práci není zpracována problematika kybernetických útoků na zdravotnická zařízení a problematika ztráty citlivých dat. Toto téma je značně rozsáhlé a jeho řešení by se mohlo stát předmětem dalšího zkoumání pro zajištění komplexní bezpečnosti zdravotnického zařízení.

9 ZDROJE

ALIBEK, Ken a Stephen HANDELMAN. *Biohazard*. Přeložil Vlastislav KOTOUČEK, přeložil Jiří ZEDNÍK, přeložil Dagmar BREJLOVÁ. Praha: Naše vojsko, 2010. ISBN 80-206-0629-7.

BRABEC, František. *Bezpečnost pro firmu, úřad, občana.* 1.vyd. Praha: Public History, 2001, 400 s. ISBN 80-864-4504-6.

ČAMBORA, Jan. Kybernetických útoků na české nemocnice přibývá, loni jich hackeři napadli pětinu. *Světchytře.cz* [online]. Praha, 18. dubna 2020 [cit. 2021-01-30]. Dostupné z: https://www.svetchytre.cz/a/p9VVM/kybernetickych-utoku-na-ceske-nemocnice-pribyva-loni-jich-hackeri-napadli-petinu

ČESKO. Ústavní zákon č. 1/1993 Sb., ústava České republiky. In: *Sbírka* zákonů. 1993

ČESKO. Usnesení č. 2/1993 Sb., předsednictva České národní rady o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součástí ústavního pořádku České republiky. In: *Sbírka zákonů*. 1993

ČESKO. Část 2 zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách). In: *Sbírka zákonů*. 2011

ČESKO. Vyhláška č. 92/2012 Sb., o požadavcích na minimální technické a věcné vybavení zdravotnických zařízení a kontaktních pracovišť domácí péče. In: *Sbírka zákonů*. 2012

ČESKO. Zákon č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů. In: *Sbírka zákonů*. 2000

ČESKO. Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon). In: *Sbírka zákonů*. 2000

ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. In: *Sbírka zákonů*. 2009

ČESKO. Část 1 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Sbírka zákonů*. 2014

ČESKO. Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád). In: *Sbírka zákonů*. 1961

ČERNÝ, Josef, IVANKA, Ján a Ústav elektrotechniky a měření. *Systemizace bezpečnostního průmyslu I*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2005. s. 52. ISBN 80-7318-310-2. Dostupné také z: https://ndk.cz/uuid/uuid:b46fa7b0-d38b-11e6-b3b6-005056825209

ČSN EN 1627. *Dveře, okna, lehké obvodové pláště, mříže a okenice - Odolnost proti vloupání - Požadavky a klasifikace*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2012.

ČSN ISO 31000. *Management rizik*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2019.

ČSN P 73 4450-1. *Fyzická ochrana prvku kritické infrastruktury - Část 1: Obecné požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

ČSN EN 50131. *Poplachové systémy - Poplachové zabezpečovací a tísňové systémy*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2018.

ČSN EN 60839-11-1. *Poplachové a elektronické bezpečnostní systémy - Část 11-1: Elektronické systémy kontroly vstupu*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

ČSN 76 1702. *Poskytovatelé bezpečnostních služeb - Fyzická ostraha*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

ČSN EN 62676-1-1. *Dohledové videosystémy pro použití v bezpečnostních aplikacích*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

ČSN EN 50131-3. *Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 3: Ústředny*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2010.

ČSN EN 1143-1. *Bezpečnostní úschovné objekty - Požadavky, klasifikace a metody zkoušení odolnosti proti vloupání - Část 1: Skříňové trezory, ATM trezory, trezorové dveře a komorové trezory*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

ČSN EN 356. *Sklo ve stavebnictví - Bezpečnostní zasklení - Zkoušení a klasifikace odolnosti proti ručně vedenému útoku*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2000.

FISCHER, Robert J. Fischer a Gion GREEN. *Introduction to Security*. 8th edition. Oxford: Elsevier, 2008. ISBN 978-0-7506-8432-3.

FOŘTL, Karel a Fakulta architektury. *Občanské stavby: stavby zdravotnické*. Praha: Vydavatelství ČVUT, 2003. s. [1a]. ISBN 80-01-02730-9. Dostupné také z: https://ndk.cz/uuid/uuid:7d82e820-b71a-11e2-b48c-001018b5eb5c

HOLUBOVÁ, Věra. *Ochrana objektů*: Studijní materiály, VŠB-TU Ostrava, Fakulta bezpečnostního inženýrství, 3. ročník.

HORÁK, Rudolf, MIKA, Otakar J. a Fakulta ekonomiky a managementu. *Ochrana obyvatelstva před terorismem.* Brno: Univerzita obrany, 2007. s. 5. ISBN 978-80-7231-295-5. Dostupné také z: https://ndk.cz/uuid/uuid:869263f1-fcdd-4b8b-a1dc-27f6d8feffe5

KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. Vyd. 3. [S.l.: s.n.], 2006 ISBN 8090293824.

LUKÁŠ, Luděk. *Teorie bezpečnosti I*. Zlín: Radim Bačuvčík - VeRBuM, 2017. s. 124. ISBN 978-80-87500-89-7. Dostupné také z: https://ndk.cz/uuid/uuid:55b727d1-4ac2-4fa8-8329-58122251dd87

MINISTERSTVO ZDRAVOTNICTVÍ ČR*: Co je krizové řízení* [online]. Praha, 2020, 20. 7. 2020 [cit. 2020-12-30]. Dostupné z: https://www.mzcr.cz/co-je-krizove-rizeni/

MINISTERSTVO VNITRA a GENERÁLNÍ ŘEDITELSTVÍ HZS. *Koncepce ochrany obyvatelstva do roku 2020 s výhledem do roku 2030*. Praha, 2013.

NEŠPOROVÁ, Veronika a Johana TAŠLOVÁ. *BEZPEČNOST ZDRAVOTNICKÉ KRITICKÉ INFRASTRUKTURY*. Žilina, 2015.

SOFT TARGETS PROTECTION INSTITUTE, Z.Ú. a Zdeněk KALVACH. *Základy ochrany měkkých cílů - metodika (1. verze)* [online]. Praha, 2016 [cit. 2021-02-23].

ŠÍN, R. et al. *Medicína katastrof*. 1. vyd. Praha: Galén, 2017, 351 s. ISBN 978-808492-295-4.

UHLÁŘ, Jan. *Technická ochrana objektů: Mechanické zábranné systémy*. Praha: Vydavatelství PA ČR, 2004. ISBN 80-725-1172-6.

UHLÁŘ, Jan. *Technická ochrana objektů: Elektrické zabezpečovací systémy*. Praha: Vydavatelství PA ČR, 2005. ISBN 80-7251-189-0.

UHLÁŘ, Jan. *Technická ochrana objektů: Ostatní zabezpečovací systémy*. Praha: Vydavatelství PA ČR, 2006. ISBN 80-7251-235-8

VOHLÍDAL, Václav. *Pacient napadl nožem personál nemocnice ve Slaném. Ochranka ho postřelila. IRozhlas* [online]. Praha, 2020, 16. 1. 2020 [cit. 2021-01-20]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/nemocnice-slane-pacient-napadeni-personalu-nuz-ochranka-strelba_2001160916_ako?fbclid=IwAR0_8Fw2Ib-VsN8OvMQZswEKHc5uWAZ4xHwm9CoiQrHsMUGYG8mWxGnPOAWs

10 SEZNAM OBRÁZKŮ

11 SEZNAM TABULEK

12 SEZNAM ZKRATEK

ARO	Anesteziologicko-resuscitační oddělení
DRNR	Doprava raněných, nemocných a rodiček
EU	Evropská unie
EZS	Elektronický zabezpečovací systém
FO	Fyzická ostraha
GŘ HZS	Generální ředitelství Hasičského záchranného sboru
IBS	Integrovaný bezpečnostní systém
IZS	Integrovaný záchranný systém
JIP	Jednotka intenzivní péče
LSPP	Lékařská služba první pomoci
LZS	Letecká záchranná služba
MZČR	Ministerstvo zdravotnictví České republiky
MZS	Mechanické zábranné systémy
ÚNMZ	Úřad pro technickou normalizaci, metrologii a státní zkušebnictví
UP	Urgentní příjem
ZZ	Zdravotnické zařízení
ZZS	Zdravotnická záchranná služba