KRÍZOVÝ MANAŽMENT
DOI 10.26552/krm.C.2025.2.99-108
ISSN – 1336 – 0019 (tlač)
ISSN – 2730 – 0544 (online)

BEZPEČNOSTNÍ OPATŘENÍ VE ZDRAVOTNICKÝCH ZAŘÍZENÍCH: ANALÝZA A DOPORUČENÍ

SECURITY MEASURES IN HEALTHCARE FACILITIES: ANALYSIS AND RECOMMENDATIONS

JITKA KOSÁČKOVÁ, RENATA HAVRÁNKOVÁ

ABSTRACT: This article addresses security measures in healthcare facilities, focusing on hospitals as soft targets exposed to increasing threats. The aim is to analyse current protection systems and propose measures to enhance resilience. Using both qualitative and quantitative methods, the research included analysis of legislation, technical standards, internal guidelines, and a comparison of security practices in selected Czech hospitals. The outcome is the MOBIZ methodology, which emphasises clear responsibilities, continuous staff training, and the involvement of all organizational levels. Pilot testing confirmed its applicability and demonstrated that an integrated approach combining technical, organisational, and human factors effectively reduces risks and strengthens resilience in healthcare facilities.

KEYWORDS: *Healthcare Facilities. Patient Safety. Security. Soft Targets.*

ÚVOD

Bezpečnost zdravotnických zařízení je nezbytným předpokladem pro poskytování kvalitní péče a ochranu pacientů, zaměstnanců i návštěvníků. Zdravotnická zařízení jsou vzhledem ke své povaze a koncentraci osob zařazovány mezi měkké cíle, což zvyšuje jejich zranitelnost vůči bezpečnostním incidentům.

Zkušenosti z posledních let potvrzují, že zdravotnická zařízení se musí systematicky připravovat na celé spektrum bezpečnostních hrozeb. Účinná bezpečnostní politika nesmí být omezena pouze na technická opatření, ale musí být založena na komplexním souboru organizačních a procesních mechanismů. Tyto mechanismy zahrnují zejména pravidelné vyhodnocování hrozeb a rizik, cyklickou odbornou přípravu zaměstnanců, průběžnou aktualizaci krizové dokumentace a realizaci taktických cvičení, jejichž výsledky slouží jako podklad pro optimalizaci preventivních a reakčních opatření. Jeho cílem je kriticky zhodnotit dosavadní opatření a formulovat doporučení, jež mohou přispět k posílení odolnosti zdravotnických zařízení vůči širokému spektru bezpečnostních hrozeb.

Cílem tohoto výzkumu bylo vytvořit jednotnou metodiku **MOBIZ – Metodika opatření pro bezpečnostní incidenty ve zdravotnictví** a stanovit komplexní rámec pro ochranu zdravotnických zařízení jako měkkých cílů před bezpečnostními hrozbami, které mohou ohrozit život, zdraví a bezpečnost pacientů, zaměstnanců i návštěvníků.

1. METODIKA VÝZKUMU

Metodologický rámec výzkumu vychází z kombinace kvalitativních a kvantitativních přístupů. Základními výzkumnými nástroji byla obsahová analýza právních předpisů, interních směrnic zdravotnických zařízení a technických norem. Tento postup umožnil systematicky zmapovat legislativní i provozní požadavky v oblasti bezpečnosti a vytvořit východisko pro návrh metodiky.

Metodika byla zpracována na základě upravených postupů uvedených v dokumentu *Základy ochrany měkkých cílů* (MV ČR, 2017) a v publikaci *Systém hodnocení bezpečnosti vybraných objektů měkkých cílů* (Mrázková & Hromada, 2019). Oba přístupy byly adaptovány na specifické podmínky zdravotnických zařízení, zejména na jejich otevřenost, provozní charakter a zranitelnost vůči cíleným bezpečnostním incidentům.

Komparativní analýza bezpečnostních opatření byla provedena v devíti nemocnicích s urgentním příjmem různé velikosti a zřizovatelské struktury. Soubor zahrnoval státní nemocnice zřizované Ministerstvem zdravotnictví ČR, velká nestátní zařízení s kapacitou nad 1 000 lůžek i menší nestátní nemocnice s kapacitou do 500 lůžek. Analýzu doplnily polostrukturované rozhovory s odborníky na krizové řízení a bezpečnostní management, které přinesly expertní perspektivu a zpřesnily interpretaci získaných dat.

Hodnocení proběhlo prostřednictvím Hospital Security Indexu (H-SI), který posuzuje fyzickou, elektronickou, mechanickou a organizačně-provozní bezpečnost. Každé dílčí kritérium bylo hodnoceno na čtyřbodové škále 0–3 (0 = nezajištěno, 1 = zajištěno nedostatečně, 2 = zajištěno uspokojivě, 3 = zajištěno plně a efektivně). Součty bodů v jednotlivých oblastech byly následně přepočteny pomocí váhových koeficientů a normalizovány na škálu 0–100, kde 0 představuje kriticky nízkou a 100 maximální dosažitelnou úroveň bezpečnosti. Výsledné hodnoty H-SI jsou dále interpretovány podle čtyř úrovní: 0–25 velmi nízká, 26–50 nízká, 51–75 střední a 76–100 vysoká úroveň bezpečnosti

2. VÝSLEDKY KOMPARATIVNÍ ANALÝZY A ROZHOVORŮ

Komparativní analýza byla provedena v devíti nemocnicích s urgentním příjmem různé velikosti (1–3 státní nemocnice, 4–6 velké nestátní nemocnice nad 1 000 lůžek, 7–9 menší nestátní nemocnice do 500 lůžek).

2.1 Souhrnné výsledky H-SI

Hodnoty H-SI se v hodnoceném souboru nemocnic pohybovaly v rozmezí od 20,9 bodu (nejnižší úroveň bezpečnosti) do 80,7 bodu (nejvyšší úroveň). Nejlépe byly hodnoceny nemocnice zřizované Ministerstvem zdravotnictví ČR, které vykazovaly vysokou míru standardizace postupů a stabilní systém řízení bezpečnosti. Naopak nejnižší hodnoty byly zaznamenány u menších nestátních nemocnic.

Tabulka 1 Souhrnné výsledky hodnocení H-SI (vlastní výzkum)

Nemocnice	Fyzická	Elektronická	Mechanická	Organizační	Celkový H-SI
1	30,0	14,1	14,6	15,6	**74,2**
2	30,0	16,7	16,7	17,3	**80,7**
3	30,0	13,0	11,5	9,3	**63,8**
4	30,0	14,1	11,5	16,0	**71,6**
5	13,3	7,8	7,3	4,4	**32,8**
6	16,7	7,8	7,3	9,8	**41,6**
7	13,3	9,9	9,4	4,4	**37,0**
8	6,7	5,7	6,3	2,2	**20,9**
9	16,7	9,4	10,4	5,3	**41,8**

2.2 Interpretace výsledků

Z výsledků vyplývá, že státní nemocnice (1–3) dosahují systematicky vyšší úrovně bezpečnosti ve všech hodnocených oblastech, zejména díky standardizovaným postupům, funkčnímu řízení bezpečnosti a pravidelnému školení personálu. Velké nestátní nemocnice (4–6) vykazují výraznou variabilitu – nemocnice 4 se blíží úrovni státních zařízení, zatímco nemocnice 5 a 6 spadají do pásma nízké bezpečnosti. Nejnižší úroveň byla zaznamenána u menších nestátních nemocnic (7–9), zejména v elektronické a organizačně-provozní oblasti.

Tato zjištění odpovídají poznatkům z polostrukturovaných rozhovorů, v nichž odborníci upozorňovali na nedostatečné pokrytí kamerovými systémy, absenci přístupových technologií, nepravidelná školení zaměstnanců, rozdílnou úroveň připravenosti na spolupráci s integrovaným záchranným systémem

(IZS), neaktuální bezpečnostní dokumentaci a zásadní roli bezpečnostního manažera v organizacích s vyšší bezpečnostní kulturou
Interpretace dat byla strukturována podle čtyř pilířů Hospital Security Indexu (H-SI). Fyzická oblast ukázala nedostatky v režimu vstupů a nastavení role ostrahy. Elektronická oblast potvrdila výrazné rozdíly v rozsahu a funkčnosti kamerových systémů a tísňových prvků. Mechanická oblast poukázala na variabilní úroveň bariér proti neoprávněnému vstupu. Organizačně-provozní oblast identifikovala největší slabiny, zejména v řízení bezpečnosti, dokumentaci a systematickém vzdělávání personálu.

Souhrnná interpretace poskytla komplexní obraz o bezpečnostní odolnosti hodnocených nemocnic a zároveň identifikovala klíčová slabá místa, která mají největší dopad na jejich schopnost reagovat na bezpečnostní incidenty. Tato zjištění byla následně zapracována do návrhu metodiky MOBIZ, kde tvoří základ struktury doporučených opatření ve fyzické, elektronické, mechanické a organizačně-provozní oblasti. Metodika tak přímo reflektuje empirické poznatky získané z komparativní analýzy a odborných rozhovorů.

Konkrétní výsledky komparativní analýzy i rozhovorů tvoří empirický základ navrhované metodiky **MOBIZ – Metodiky opatření pro bezpečnostní incidenty ve zdravotnictví** a jsou podrobně prezentovány v následující části.

3. MOBIZ – METODIKA OPATŘENÍ PRO BEZPEČNOSTNÍ INCIDENTY VE ZDRAVOTNICTVÍ

Metodika MOBIZ vymezuje metodický rámec prevence a zvládání bezpečnostních incidentů ve zdravotnických zařízeních. Zaměřuje se na právní a strategické dokumenty, bezpečnostní plán, analýzu bezpečnostních prvků a doporučení pro praxi. Metodika vychází z legislativy a technických norem a je přizpůsobena specifickým podmínkám prostředí zdravotnických zařízení.

3.1 Dokumentace ochrany měkkých cílů

Právní rámec ochrany zdravotnických zařízení jako měkkých cílů vychází z platných zákonů, prováděcích vyhlášek, strategických a koncepčních dokumentů České republiky, interní dokumentace jednotlivých zdravotnických zařízení a závazných technických norem. Jeho účelem je vymezit povinnosti subjektů v oblasti prevence, připravenosti a reakce na bezpečnostní incidenty, které mohou ohrozit život, zdraví či osobní bezpečnost pacientů, zaměstnanců a dalších osob přítomných v prostředí zdravotnických zařízení.

Ukotvení problematiky měkkých cílů v bezpečnostním prostředí České republiky ukazuje, že stát si je vědom rizik spojených s ochranou těchto objektů a usiluje o jejich systematickou ochranu a prevenci možných útoků. V této souvislosti jsou vyvíjeny snahy o posílení prevence, zvýšení úrovně ochrany a zlepšení schopnosti reakce na teroristické hrozby (Jakubcová a kol., 2018).

Zásadním dokumentem bezpečnostní politiky státu je Bezpečnostní strategie České republiky 2023, která navazuje na předchozí strategické a koncepční materiály. Jejím cílem je prosazovat bezpečnostní zájmy ČR prostřednictvím systémového a koordinovaného přístupu a účinně využívat multilaterální, bilaterální i národní nástroje k řízení bezpečnostního prostředí a k efektivní alokaci zdrojů (Česká republika, 2023).

Na tuto strategii navazuje Koncepce ochrany měkkých cílů pro roky 2017–2020, jejímž cílem bylo vytvořit fungující národní systém ochrany měkkých cílů umožňující pružně a komplexně reagovat na vznikající hrozby (MV ČR, 2017). V rámci její implementace vydává ministerstvo vnitra řadu metodických materiálů, jako např. Metodiku koordinace měkkého cíle pro fáze po závažném incidentu, Vyhodnocení ohroženosti měkkého cíle či Bezpečnostní plán měkkého cíle, které jsou veřejně dostupné (MV ČR, 2025).

Dalším významným dokumentem je Strategie pro boj proti terorismu od roku 2013, vydaná Ministerstvem vnitra ČR, která zdůrazňuje prevenci a ochranu měkkých cílů, analyzuje teroristické

hrozby a identifikuje ohrožené objekty v ČR. Jejím hlavním cílem je posílit schopnost státu reagovat na teroristické útoky a minimalizovat jejich dopady na společnost (MV ČR, 2013).

Česká republika zároveň podporuje a implementuje evropské strategické dokumenty, zejména Evropskou bezpečnostní strategii: Bezpečná Evropa v lepším světě (Rada EU, 2003) a Evropskou strategii vnitřní bezpečnosti – ProtectEU (Evropská komise, 2025), které akcentují význam prevence terorismu a systematické ochrany měkkých cílů.

Klíčovým technickým dokumentem v oblasti zdravotnictví je ČSN P CEN/TS 16850 – Ochrana společnosti: pokyny pro řízení bezpečnosti ve zdravotnických zařízeních. Tato norma poskytuje komplexní rámec pro řízení bezpečnosti zdravotnických zařízení. Definuje postupy pro ochranu osob, identifikaci a zabezpečení kritických procesů, stanovuje požadavky na bezpečnostní vybavení, školení personálu i úpravu prostor pro rizikové pacienty. Je přizpůsobena specifikům různých typů zařízení, včetně zdravotnických zařízen, zařízení sociální péče a léčeben, a její pokyny vytvářejí základní systém řízení bezpečnosti v celém resortu (ČSN P CEN/TS 16850, 2020).

Při posouzení ohrožení je však klíčové vědět, co je třeba chránit, proti komu jsou tyto hodnoty chráněny a jakým způsobem mohou hrozby na zdroje působit (Kalvach, 2016). Skutečné zvýšení bezpečnosti měkkých cílů proto nelze zajistit pouze právními předpisy, ale především faktickými preventivními a reaktivními opatřeními organizačního, technického i komunikačního charakteru.

3.2 Bezpečnostní plán a resilience zdravotnických zařízení

Resilience zdravotnických zařízení je podmíněna komplexním souborem bezpečnostních opatření, jejichž cílem je chránit pacienty, zaměstnance i návštěvníky a zajistit kontinuitu poskytované péče. Podle Ministerstva vnitra ČR (2025) je klíčovým nástrojem této ochrany **bezpečnostní plán**, který umožňuje řídit preventivní, přípravná i reakční opatření a tím minimalizovat dopady násilných útoků či mimořádných událostí.

Tento plán se opírá o čtyři základní dimenze bezpečnostních prvků – **fyzickou, elektronickou, mechanickou a organizačně-provozní**. Jejich vzájemná provázanost určuje schopnost zdravotnického zařízení účinně čelit incidentům a minimalizovat jejich dopady. Aby však mohl plán plnit svou roli, je nezbytné, aby organizace dokázala systematicky identifikovat a vyhodnocovat rizikové situace a přijímat na jejich základě odpovídající opatření. Klíčovou roli v tomto procesu hraje **bezpečnostní manažer** či jiný pověřený pracovník, který odpovídá za oblast bezpečnosti, koordinuje implementaci plánu a zajišťuje komunikaci s Policií ČR a dalšími složkami IZS (Kalvach a kol., 2016).

3.2.1 Bezpečnostní plán zdravotnického zařízení

Bezpečnostní plán je klíčovým nástrojem posilování resilience zdravotnických zařízení, protože zajišťuje kontinuitu péče i při mimořádných událostech. Kalvach a kol. (2016) ve své metodice zdůrazňuje nutnost zaměřit se při ochraně měkkých cílů na organizační strukturu, která zajišťuje formulaci a realizaci bezpečnostní politiky, zpracování bezpečnostního plánu a řízení konkrétních opatření.

Užitečný metodický rámec pro tvorbu a pravidelnou revizi bezpečnostního plánu nabízí metoda **PDCA** (Plan–Do–Check–Act – naplánuj, proveď, zkontroluj, jednej). Ve svém článku ji Zelenák & Kyselák (2024) představují jako praktický nástroj, který zdravotnickým zařízením umožňuje systematicky plánovat opatření, uvádět je do praxe, vyhodnocovat jejich účinnost a následně provádět úpravy na základě získaných zkušeností. Tímto způsobem lze zajistit, aby plán zůstal dlouhodobě funkční a odrážel aktuální hrozby i provozní podmínky.

S ohledem na charakter zdravotnického zařízení jako měkkého cíle se doporučuje, aby měl plán podobu strukturovaného dokumentu reflektujícího legislativní rámec, specifika provozu i aktuální bezpečnostní hrozby. Standardně se člení do čtyř částí: základní, operativní, pomocné a přílohové. Základní část vymezuje účel, cíle, právní rámec, odpovědnosti i způsoby zajištění akceschopnosti zdravotnického zařízení. Operativní část obsahuje konkrétní postupy řešení mimořádných událostí, svolání krizového štábu, aktivace zaměstnanců a typové scénáře. Její aktuálnost je třeba ověřovat pravidelnými cvičeními.

Pomocná část poskytuje podpůrné nástroje, přehled kontaktů, grafické podklady a související dokumentaci. Přílohová část pak nabízí přehled rizik a vzorové postupy pro řešení vybraných scénářů, například útoku aktivního střelce, výhružného telefonátu, nálezu podezřelého předmětu, jednání s agresivní osobou či použití nebezpečných chemických, biologických, radiačních, jaderných a výbušných látek (CBRNE) (MV ČR, 2025).

Bezpečnostní plán je nutné chápat jako živý dokument, který se pravidelně reviduje, testuje a přizpůsobuje aktuálním podmínkám. Jeho efektivní implementace posiluje bezpečnostní kulturu organizace a zvyšuje její schopnost reagovat na mimořádné situace. Součástí plánu by měl být také přehled dostupných sil a prostředků, jak organizačních a personálních, tak technických (mechanických i elektronických), a jasné vymezení jejich role v prevenci i při řešení incidentu (MV ČR, 2025).

Právě fyzická bezpečnost tvoří první z těchto pilířů a zároveň praktické naplnění bezpečnostního plánu v každodenním provozu zdravotnického zařízení.

3.2.2 Fyzická bezpečnost

Fyzická bezpečnost je základním pilířem ochrany prostředí zdravotnických zařízení a významně přispívá k jejich celkové resilienci. Jejím jádrem je činnost **bezpečnostní služby (ostrahy)**, která jako jediná složka systému dokáže bezprostředně zasáhnout při hrozícím nebo probíhajícím incidentu. Primárním cílem ostrahy je ochrana osob, majetku a kontinuity zdravotní péče (ČSN P CEN/TS 16850, 2020). Opatření zahrnují fyzickou kontrolu osob vstupujících do areálu, sledování nezvyklého chování, inspekci zavazadel a prevenci vnášení nebezpečných předmětů (Nevrkla & Lapková, 2017). Pracovníci ostrahy provádějí kontrolu vstupu, pochůzkovou činnost nebo obsluhují velín a bezpečnostní technologie. Výkon služby musí být zajištěn nepřetržitě (24/7) – buď prostřednictvím vlastních zaměstnanců zdravotnického zařízení, externí bezpečnostní agentury nebo kombinací obou variant (MV ČR, 2025).

Nedílnou součástí fyzické bezpečnosti jsou pravidelná školení a cvičení. Musí zahrnovat simulace násilných incidentů, nácvik evakuace a koordinační cvičení se složkami IZS. Doporučuje se je realizovat alespoň jednou ročně a jejich výsledky využívat k aktualizaci vnitřních postupů. Obsah školení je třeba průběžně přizpůsobovat aktuálním hrozbám a zapojit do něj všechny pracovníky ostrahy. Činnost ostrahy má být přesně vymezena standardizovanými postupy, které tvoří součást bezpečnostní dokumentace zařízení. Ta zahrnuje plán ostrahy, směrnice pro výkon služby, provozní režimy objektů a závazné postupy pro řešení incidentů. Pouze jejich důsledná aplikace zajistí připravenost zařízení a posílí jeho bezpečnostní kulturu (Kalvach a kol., 2016).

Dalším prvkem bezpečnostního plánu jsou **režimová opatření** – interní pravidla upravující chování zaměstnanců v rámci objektu. Definují postupy pro vstup do budovy, pravidla pro vjezd vozidel, obsluhu elektronických bezpečnostních systémů a další každodenní činnosti (ČSN P 73 4450-1, 2013).

Jak již bylo zmíněno, mezi prostředky k ochraně měkkých cílů patří **technická bezpečnostní opatření** (Tabulka 1). Pouhá existence technických bezpečnostních opatření není postačující. Je nezbytné mít vytvořené standardizované procedury a postupy, které stanoví, jak tato opatření budou používána a jak budou vyhodnocována (Kalvach a kol., 2016; ČSN P CEN/TS 16850, 2020).

Tabulka 2 Technická bezpečnostní opatření (Kalvach a kol., 2016)

Technická bezpečnostní opatření	
Elektronické prvky	**Mechanické prvky**
Kamerový systém	Double door
Poplachové zabezpečovací a tísňové systémy	Ploty, zdi
Vnitřní rozhlas	Bezpečnostní okna
Rentgen	Zátarasy
Přístupové a docházkové systémy	Mříže a okenice
Další	Další

3.2.3 Elektronické prvky bezpečnosti ve zdravotnických zařízeních

Elektronické bezpečnostní prvky představují klíčovou součást komplexního systému ochrany zdravotnických zařízení. Základním opatřením je **kamerový dohled**, který musí zajišťovat nepřetržité monitorování obvodu budovy bez slepých míst. Záznamy je vhodné uchovávat minimálně 24 hodin, ideálně 72 hodin, přičemž kamery by měly být vybaveny nočním viděním a detekcí pohybu pro efektivní provoz i za zhoršených světelných podmínek (ČSN EN 62676-1-1, 2014; Kalvach a kol., 2016).

Účinnost kamerového systému je podmíněna řízeným vstupem do objektu. Během provozní doby by měl být vstup kontrolován fyzickou ostrahou, mimo provoz pak zajištěn elektronickými systémy. Vstupní body je žádoucí doplnit o rentgenová zařízení a detektory kovů či výbušnin, které zabraňují vnášení nebezpečných předmětů. Pozornost je třeba věnovat také okolí zdravotnického zařízení – parkoviště má být monitorováno kamerovým systémem, záznam by měl být uchováván alespoň 12 hodin, což umožňuje zpětnou kontrolu pohybu osob i vozidel. Nedílnou součástí ochrany jsou **poplachové zabezpečovací a tísňové systémy** (PZTS), které je vhodné instalovat ve všech budovách a napojit na dohledové a poplachové přijímací centrum (DPPC). To musí zajišťovat nepřetržitý monitoring a být schopno detekovat podezřelé chování, neoprávněný pohyb či výskyt odložených předmětů. Na rizikových pracovištích je účelné doplnit systém o tísňová tlačítka pro rychlé a skryté přivolání pomoci, přičemž provoz DPPC má být svěřen kvalifikovanému personálu (ČSN EN 50131-1, 2007; Kalvach a kol., 2016)

Neméně důležitou součástí elektronické ochrany je vnitřní rozhlas, který slouží jako klíčový nástroj krizové komunikace. Instalace ve všech prostorách zdravotnického zařízení umožňuje efektivní informování osob při mimořádných událostech. Pro dosažení maximální účinnosti má být systém propojen s **elektrickou požární signalizací** (EPS) podle normy ČSN EN 54-16 (2009). Tím lze okamžitě přenést varovné hlášení nebo příkaz k evakuaci do celého objektu, což významně zkracuje reakční dobu a posiluje ochranu pacientů i zaměstnanců. Tento systém je vhodné doplnit o detekční zařízení, například rentgeny či detektory kovů a výbušnin, instalovaná u hlavních vstupů za účelem prevence vnášení nebezpečných předmětů (Kalvach a kol., 2016).

Významnou roli hrají také systémy kontroly vstupu. **Elektronický systém kontroly osob** (EASC) je vhodné implementovat v celém objektu a integrovat s ostatními bezpečnostními prvky. Tento systém umožňuje blokaci či uvolnění přístupových bodů podle aktuální situace a jeho funkčnost je nutné pravidelně testovat (ČSN EN 60839-11-1, 2014). Přístupové mechanismy mezi jednotlivými místnostmi je pak žádoucí doplnit o elektronické uzamykací prvky dle normy ČSN EN 1627 a nastavovat oprávnění v závislosti na rizikovosti konkrétních prostor (Vyhláška č. 528/2005 Sb., 2005; ČSN EN 1627, 2022).

Doplňujícím prvkem mohou být čtečky dokladů, které je účelné instalovat na vybraných místech a integrovat do přístupového systému za účelem ověřování totožnosti osob. Současně je vhodné zajistit funkční **systém šíření varování** prostřednictvím specializovaných krizových a notifikačních platforem, například O_2 KISS, Everbridge či BlackBerry AtHoc, doplněných o informační panely, SOS tlačítka a geolokační cílení zpráv. Osvětlení s pohybovými čidly je účelné umístit do exponovaných prostor a propojit s kamerovým dohledem a poplachovými systémy (Kalvach a kol., 2016). Individuální bezpečnostní ochranu pak představují prostředky určené přímo pro personál – zejména na rizikových pracovištích je vhodné zaměstnance vybavit **elektronickými bezpečnostními náramky** nebo SOS tlačítky pro okamžité přivolání pomoci. Signál má být směrován přímo na bezpečnostní službu nebo dispečink zdravotnického zařízení, a to v souladu s ČSN CEN/TS 16850 (2020) jako součást systému řízení bezpečnosti.

3.2.4 Mechanické prvky zabezpečení zdravotnických zařízení

Druhou skupinu technických bezpečnostních systémů, kterou je nutno zmínit, jsou **mechanické prvky,** které tvoří základní vrstvu bezpečnosti zdravotnického zařízení. Jejich správné navržení a implementace významně přispívají k ochraně před neoprávněným vstupem, násilným vniknutím a jinými bezpečnostními incidenty.

Exteriérové dveře je vhodné vybavit uzamykatelným bezpečnostním zámkem a konstruovat je tak, aby odpovídaly požadavkům na zvýšenou mechanickou odolnost dle normy ČSN EN 1627 (2022). Pro vyšší účinnost se doporučuje jejich propojení s elektronickými prvky – kamerovým dohledem, čipovým přístupem či biometrickým ověřováním. V případě mimořádné události musí být zajištěna možnost nouzového uzamčení objektu. Kvalitní bezpečnostní dveře dokážou odolat výbuchu, střelbě či násilným pokusům o vniknutí a spolu s přístupovými systémy tvoří účinný nástroj pro kontrolu vstupu (Kalvach a kol., 2016). Neméně významná jsou **bezpečnostní okna**, která se vyrábějí v různých třídách odolnosti – proti střelbě, výbuchu či prohození předmětů. Jejich funkčnost však závisí na správném ukotvení do nosných stěn. Alternativní ochranu mohou poskytnout těžké závěsy zvyšující odolnost proti tlakové vlně (ČSN P CEN/TS 16850, 2020; ČSN EN 1627, 2022)

Důležitou roli hrají také **režimová opatření** při vjezdu do areálu. Vstup vozidel je vhodné regulovat závorami, automatickým rozpoznáváním registračních značek a kamerovým systémem. Přístup lze omezit fyzickými překážkami – zábradlím, pevnými sloupky či zelení – které zamezují nájezdu vozidel mimo vyhrazené trasy. Celý areál by měl být ohraničen oplocením vysokým minimálně dva metry, přičemž vstupní brány mají být uzamykatelné a napojené na kontrolní systémy (Kalvach a kol., 2016).

Další specifickou kategorii tvoří **fyzické bariéry** – například turnikety, vstupní zábrany nebo pevné bloky. Tyto prvky umožňují regulaci pohybu osob a vozidel, přičemž jejich konstrukce musí respektovat požadavky na bezbariérovost a bezpečný provoz. Současně mají být integrovány do přístupového systému zdravotnického zařízení. Dle Kalvacha a kol. (2016) se za důležitý doplňkový prvek ochrany považují pevné sloupky, betonové bloky či výsuvné patníky, které mají být instalovány zejména v kritických zónách – u hlavních vstupů, zásobovacích tras či urgentního příjmu. Jejich funkcí je zabránit vjezdu nepovolaných vozidel a omezit přístup neoprávněných osob, aniž by narušovaly provoz zdravotnického zařízení (ČSN CEN/TS 16850, 2020).

Mechanické prvky tedy tvoří pevný základ fyzické ochrany. Jejich účinnost je však podmíněna správným nastavením organizačně-provozních opatření, která propojují technické prostředky s každodenním chodem zdravotnického zařízení.

3.2.5 Organizačně-provozní opatření

Součástí bezpečnostního řízení zdravotnického zařízení je soubor **organizačně-provozních opatření**, jejichž cílem je posílení odolnosti vůči bezpečnostním hrozbám a zajištění provozní kontinuity v krizových situacích.

Zdravotnické zařízení by mělo disponovat **dokumentací zaměřenou na ochranu měkkých cílů**, která se pravidelně aktualizuje v návaznosti na identifikované rizikové faktory. Tato dokumentace má být začleněna do strategického plánování a bezpečnostní politiky organizace. Pro zajištění krizové připravenosti se doporučuje zpracování souboru dokumentů, zahrnujícího plán krizové připravenosti, požární poplachové plány, evakuační plán, pandemický plán, havarijní plán, traumatologický plán a další provozní směrnice. Obsah těchto dokumentů má odpovídat platné legislativě a provozním specifikům daného zařízení (MV ČR, 2025).

Klíčovou roli hraje zapojení zaměstnanců. Ti se mají pravidelně účastnit **školení** zaměřených na krizovou dokumentaci a praktické zvládání mimořádných událostí. Vedoucí pracovníci se soustředí na řízení incidentů a koordinaci zásahů, zatímco ostatní zaměstnanci absolvují výuku přizpůsobenou charakteru pracoviště a míře rizika. Doporučená jsou rovněž **taktická cvičení**, která je vhodné realizovat minimálně jednou ročně ve spolupráci se složkami IZS. Tím se posiluje připravenost personálu i celková bezpečnostní kultura organizace (Kalvach a kol., 2016).

Součástí prevence je také pravidelná **analýza hrozeb a rizik**. Výstupy těchto analýz slouží jako podklad pro aktualizaci bezpečnostních postupů, plánování školení a provádění cvičení. Jejich systematické využívání podporuje dlouhodobé zvyšování resilience organizace (Kalvach, 2025).

Organizačně-provozní opatření se tak stávají mostem mezi technickými prvky a každodenním fungováním zdravotnického zařízení. Na jejich základě vzniká bezpečnostní politika, která sjednocuje pravidla, vymezuje odpovědnosti a určuje rámec spolupráce s externími složkami.

3.2.6 Bezpečnostní politika zdravotnického zařízení

Efektivní řízení bezpečnosti vyžaduje jasně definovanou bezpečnostní politiku, která stanovuje odpovědnosti, pravidla a rámec koordinace. Klíčovým prvkem je ustanovení bezpečnostního manažera, jenž zajišťuje vyhodnocování rizik, aktualizaci plánů, organizaci školení a komunikaci se složkami IZS. Součástí jeho role je také vyhodnocování bezpečnostních incidentů a dohled nad implementací metodiky ochrany měkkých cílů (Kalvach a kol., 2025).

Bezpečnostní politika však musí zahrnovat i zapojení všech zaměstnanců. Neodborný personál má být školen v rozpoznávání podezřelých osob, předmětů či situací a v základních postupech v případě mimořádných událostí. Školení se přizpůsobuje specifikům jednotlivých pracovišť a klade důraz na prevenci, rychlou reakci a spolupráci s IZS (Kalvach a kol., 2016).

Pro sjednocení postupů je třeba zavést standardizované procedury, písemně zpracované a pravidelně aktualizované. Mezi klíčové oblasti patří:

- režim vstupu osob do objektu (identifikace, autorizace a kontrola zaměstnanců, pacientů, návštěvníků i externích osob);
- režim vjezdu vozidel do areálu (podmínky pro služební, dodavatelská i návštěvnická vozidla) (Kalvach a kol., 2016).

Další součástí politiky je tematický plán školení a koordinační plán managementu, který jasně určuje úkoly vedení zdravotnického zařízení při mimořádné události a vymezuje odpovědnosti členů krizového štábu. Jeho funkčnost je nutné ověřovat modelovými situacemi (Ben David, 2025).

Bezpečnostní politika má rovněž zahrnovat aktivní spolupráci s Policií ČR, Hasičským záchranným sborem ČR, zdravotnickou záchrannou službou a obecní policií. Těmto složkám se doporučuje nabídnout možnost prohlídky objektu, zapojit je do plánování veřejných akcí, konzultovat analýzu ohroženosti a informovat je o mimořádných událostech. Pravidelná komunikace a koordinace postupů přispívají k efektivnímu zvládání mimořádných situací (Kalvach a kol., 2025).

V neposlední řadě se doporučuje navázat partnerskou spolupráci s dalšími měkkými cíli v regionu, jako jsou školy, kulturní instituce, úřady či obchodní centra. Společná opatření, výměna informací, vzájemné varování při výskytu hrozeb a pořádání cvičení zaměřených na krizové scénáře mohou významně přispět k posílení bezpečnostní připravenosti nejen zdravotnického zařízení , ale i širšího okolí (Kalvach a kol., 2016).

Závažným útokům je těžké čelit, když již nastanou, proto je důležité mít připravená opatření pro prevenci a zmírnění dopadů. Znalost místního prostředí je klíčovým faktorem, který dává personálu výhodu při plnění bezpečnostních úkolů. Místní personál má lepší povědomí o běžném chování a rutinách v daném prostředí. Personál musí být obeznámen s místními sociokulturními normami a může snáze rozpoznat neobvyklé chování nebo situace, které by jinak mohly uniknout pozornosti (Kalvach a kol., 2018).

Je nutné zmínit, že důkladné vyšetření každého incidentu má za cíl vyvodit odpovídající důsledky a zlepšit preventivní opatření. Poučení z každé události by mělo sloužit jako podklad pro lepší prevenci v budoucnosti (Háva, 2004).

3.3 Doporučení pro zdravotnická zařízení

Na základě provedené analýzy lze formulovat tato klíčová doporučení pro posílení bezpečnostní resilience zdravotnických zařízení:

- **Pravidelná revize bezpečnostního plánu** – udržovat plán jakožto živý dokument, pravidelně jej testovat a přizpůsobovat aktuálním hrozbám a provozním podmínkám.
- **Aktualizace krizové dokumentace** – průběžně doplňovat evakuační, havarijní, pandemické, traumatologické a další plány, aby odpovídaly legislativním požadavkům a provozním specifikům zařízení.
- **Posilování fyzické bezpečnosti** – zajišťovat nepřetržitou činnost ostrahy, jasně definovat její postupy a pravidelně realizovat školení a cvičení zaměřená na řešení mimořádných událostí.
- **Rozvoj technických opatření** – efektivně kombinovat elektronické (kamerové systémy, PZTS, přístupové systémy) a mechanické prvky (dveře, okna, bariéry), přičemž jejich využívání má být zakotveno ve standardizovaných postupech.
- **Systematické vzdělávání a cvičení personálu** – zajišťovat pravidelná školení všech zaměstnanců, včetně taktických cvičení se složkami IZS, s důrazem na praktické dovednosti a krizovou komunikaci.
- **Organizačně-provozní opatření** – nastavit jasná pravidla pro vstup osob, vjezd vozidel a každodenní provozní režim, která podporují prevenci incidentů a kontinuitu péče.
- **Rozvoj spolupráce a standardizace postupů** – posilovat partnerství s IZS a dalšími institucemi v regionu, sdílet zkušenosti, využívat dotační programy a zavádět jednotné bezpečnostní postupy vymezující kompetence a odpovědnosti.

ZÁVĚR

Analýza potvrzuje, že zdravotnická zařízení představují vysoce exponované měkké cíle, jejichž ochrana vyžaduje komplexní a integrovaný přístup. Účinná bezpečnostní strategie musí propojit fyzická a technická opatření s organizačními mechanismy, systematickou krizovou připraveností, pravidelným vzděláváním zaměstnanců a úzkou spoluprací se složkami IZS. Bezpečnostní plán je nutné chápat jako dynamický dokument, který se průběžně reviduje, testuje a přizpůsobuje aktuálním hrozbám i provozním podmínkám. Výsledky komparativní analýzy ukazují, že zásadním předpokladem bezpečnostní resilience je rovnováha mezi prevencí, včasnou reakcí a schopností organizace adaptovat se na měnící se rizika.

Navržená metodika MOBIZ představuje praktický nástroj pro jednotné řízení bezpečnosti v nemocnicích. Její pilotní ověření v Nemocnici České Budějovice a.s. prokázalo využitelnost v podmínkách velké krajské nemocnice, zejména při tvorbě bezpečnostního plánu a typových karet činností. Metodika má potenciál stát se sjednocujícím rámcem i pro další zdravotnická zařízení.

Studie je limitována velikostí výzkumného souboru (devět nemocnic v ČR) a částečnou subjektivitou hodnocení vyplývající z použití indexu a rozhovorů. Do budoucna by bylo vhodné rozšířit výzkum na širší vzorek nemocnic, případně mezinárodně, a dále rozvíjet softwarovou aplikaci podporující automatizované vyhodnocování H-SI a řízení bezpečnostních opatření.

LITERATURA

Ben David, G. (2025). *Metodika koordinace měkkého cíle pro fáze po závažném incidentu: aneb jak se vyrovnat s nastalou závažnou situací*. Ministerstvo vnitra České republiky, Odbor bezpečnostní politiky.

Česká republika. (2023). *Bezpečnostní strategie České republiky 2023*. Ministerstvo zahraničních věcí ČR. https://mzv.gov.cz/file/5161086/Bezpecnostni_strategie_2023.pdf (cit. 29. 9. 2025)

ČSN EN 1627. (2022). *Dveře, okna, lehké obvodové pláště, mříže a okenice – Odolnost proti vloupání – Požadavky a klasifikace*. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

ČSN EN 50131-1. (2007). *Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 1: Systémové požadavky*. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

ČSN EN 54-16. (2009). *Elektrická požární signalizace – Část 16: Ústředny pro hlasová výstražná zařízení*. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

ČSN EN 60839-11-1. (2014). *Poplachové a elektronické bezpečnostní systémy – Část 11-1: Elektronické systémy kontroly vstupu – Požadavky na systém a komponenty*. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

ČSN EN 62676-1-1. (2014). *Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 1-1: Systémové požadavky – Obecně*. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

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

ČSN P CEN/TS 16850. (2020). *Ochrana společnosti – Pokyny pro řízení bezpečnosti ve zdravotnických zařízeních*. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

Evropská komise. (2025). *Evropská strategie vnitřní bezpečnosti – ProtectEU*. Evropská komise.

Háva, P. (2004). *Násilí na pracovišti v oblasti zdravotnických a sociálních služeb v ČR: Vstupní teoretická studie*. Institut zdravotní politiky a ekonomiky.

Jakubcová, L., a kol. (2018). Měkké cíle v pojetí Hasičského záchranného sboru České republiky. In *Měkké cíle a jejich ochrana*. Policejní akademie České republiky v Praze.

Kalvach, Z. (2016). *Metodika pro zvýšení ochrany měkkých cílů*. Ministerstvo vnitra České republiky.

Kalvach, Z. (2025). *Vyhodnocení ohroženosti měkkého cíle: aneb co, kdy, kde a od koho vám hrozí* (2. vyd.). Ministerstvo vnitra České republiky, Odbor bezpečnostní politiky. https://mv.gov.cz/chh/clanek/terorismus-web-dokumenty-dokumenty.aspx (cit. 28. 9. 2025)

Kalvach, Z., a kol. (2016). *Základy ochrany měkkých cílů: Metodika*. Ministerstvo vnitra České republiky.

Ministerstvo vnitra České republiky. (2013). *Strategie České republiky pro boj proti terorismu od roku 2013*. https://mv.gov.cz/soubor/strategie-ceske-republiky-pro-boj-proti-terorismu-pdf.aspx (cit. 28. 9. 2025)

Ministerstvo vnitra České republiky. (2016). *Ochrana měkkých cílů*. https://www.mvcr.cz/clanek/ochrana-mekkych-cilu.aspx (cit. 29. 9. 2025)

Ministerstvo vnitra České republiky. (2017). *Koncepce ochrany měkkých cílů pro roky 2017–2020*. https://www.mvcr.cz/soubor/koncepce-ochrany-mekkych-cilu-2017-2020.aspx (cit. 29. 9. 2025)

Ministerstvo vnitra České republiky. (2025). *Metodické materiály k ochraně měkkých cílů*. https://www.mvcr.cz (cit. 29. 9. 2025)

Ministerstvo vnitra České republiky, Odbor bezpečnostní politiky. (2025). *Bezpečnostní plán měkkého cíle* (2. upravené vyd.). Ministerstvo vnitra ČR.

Mrázková, L., & Hromada, M. (2019). *Ochrana měkkých cílů: Systém hodnocení bezpečnosti vybraných objektů měkkých cílů*. Leges.

Nevrkla, J., & Lapková, D. (2017). *Metodika ochrany měkkých cílů*. Soft Targets Protection Institute, z. ú., Univerzita Tomáše Bati ve Zlíně.

Rada Evropské unie. (2003). *Evropská bezpečnostní strategie: Bezpečná Evropa v lepším světě*. Rada EU.

Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků. (2005). *Sbírka zákonů České republiky*.

Zelenák, M., & Kyselák, J. (2024). Bezpečnost zdravotnických zařízení. *Krizový manažment, 23*(2), 28–37. https://doi.org/10.26552/krm.C.2024.2.28-37

Jitka Kosáčková, Mgr.

Nemocnice České Budějovice a.s., B. Němcové 585/54, České Budějovice, Česká republika

ČVUT v Praze, Fakulta biomedicínského inženýrství, Katedra zdravotnických oborů a ochrany obyvatelstva, Sportovců 2311, Kladno, Česká republika

e-mail: kosackova.jitka@nemcb.cz

Renata Havránková, Mgr., Ph.D.

ČVUT v Praze, Fakulta biomedicínského inženýrství, Katedra zdravotnických oborů a ochrany obyvatelstva, Sportovců 2311, 272 01 Kladno, Česká republika

Jihočeská univerzita v Českých Budějovicích, Zdravotně sociální fakulta, Ústav radiologie, toxikologie a ochrany obyvatelstva, J. Boreckého 1167/27, 370 11 České Budějovice, Česká republika

e-mail: renata.havrankova@fbmi.cvut.cz