VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

BEZPEČNOSTNÍ VÝZNAM ZÁKLADNÍCH VNITŘNÍCH PŘEDPISŮ PRO PROVOZOVÁNÍ SYSTÉMŮ TECHNICKÉ OCHRANY OBJEKTŮ V ORGANIZACÍCH ŘÍZENÝCH ČESKÝM STÁTEM

Autor práce: Bohumil Čochnář
Studijní obor: Bezpečnostně právní činnost ve veřejné správě
Forma studia: Kombinovaná
Vedoucí práce: Mgr. Štěpán Strnad, Ph.D.
Katedra: Katedra právních oborů a bezpečnostních studií

2022

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 6, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Bohumil Čochnář

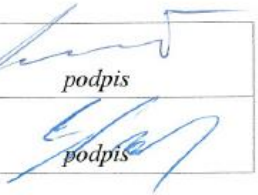
Studijní program: Bezpečnostně právní činnost
Studijní obor: Bezpečnostně právní činnost ve veřejné správě
Forma studia: Kombinovaná
Místo studia: Příbram

Název bakalářské práce:
Bezpečnostní význam základních vnitřních předpisů pro provozování systémů technické ochrany objektů v organizacích řízených českým státem

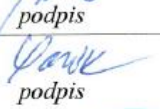
Název bakalářské práce v anglickém jazyce:
Safety Value of Basic Internal Regulations for Operation of Technical Protection Systems for Buildings in Organizations Managed by the Czech State

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce: Mgr. Štěpán Strnad, PhD.
Datum zadání bakalářské práce: březen 2021

Cíl bakalářské práce: Cílem BP je analýza bezpečnostního významu základních vnitřních předpisů systémů technické ochrany objektů v organizacích řízených českým státem. Vedlejším cílem bude autorův návrh dokumentů, vnitřních bezpečnostních předpisů pro provozování systémů technické ochrany v dané oblasti.

Student: Bohumil Čochnář	15.12.2021 *datum*	 *podpis*
Vedoucí práce: Mgr. Štěpán Strnad, PhD.	28.1.22 *datum*	 *podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	31.1.2022 *datum*	 *podpis*
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	31.1.2022 *datum*	 *podpis*
Rektor: doc. Ing. Jiří Dušek, Ph.D.	31.1.2022 *datum*	 *podpis*

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucího a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucímu bakalářské práce Mgr. Štěpánu Strnadovi, Ph.D. za jeho cenné odborné rady a metodické vedení, které mi pomohlo tuto diplomovou práci dokončit. Současně bych chtěl poděkovat respondentům, kteří mi ochotně poskytli rozhovor a manažerům bezpečnosti za vyplnění dotazníku.

ABSTRAKT

ČOCHNÁŘ, B. *Bezpečnostní význam základních vnitřních předpisů pro provozování systémů technické ochrany objektů v organizacích řízených českým státem: bakalářská práce.* České Budějovice: Vysoká škola evropských a regionálních studií, 2022. 59 s. Vedoucí bakalářské práce: Mgr. Štěpán Strnad, Ph.D.

Klíčová slova: systémy technické ochrany, vnitřní bezpečnostní předpisy

Práce se zaměřuje na aplikaci bezpečnostní politiky ve státních organizacích s cílem objasnit význam vnitřních bezpečnostních předpisů v oblasti zajišťování bezpečnosti objektů v rámci systémů technické ochrany. Smyslem je upozornit na neexistující právní akt pro bezpečnostní management, který by standardizoval rámec vnitřních bezpečnostních předpisů v organizacích řízené českým státem při ochraně zaměstnanců, včetně ochrany nehmotných aktiv a nemovitého majetku s ohledem na platné právní akty v oblasti BOZP a PO.

ABSTRACT

ČOCHNÁŘ, B. *Safety Value of Basic Internal Regulations for Operation of Technical Protection Systems for Buildings in Organizations Managed by the Czech* State: Bachelor Thesis. České Budějovice: The College of European and Regional Studies, 2022. 59 p. Supervisor: Mgr. Štěpán Strnad, Ph.D.

Key words: technical protection systems, internal safety regulations.

The dissertation focuses on the application of security policy in state organizations in order to clarify the importance of internal security regulations in the field of providing the security of buildings within the systems of technical protection. The purpose is to draw attention for protection of employees, including the protection of intangible assets and real estate with regard to applicable legal acts in the field of Occupational Safety and Health (OSH) and Fire Protection (FP).

Obsah

Úvod

Lidstvo má od nepaměti snahu jakýmkoliv způsobem ochránit a zabezpečit svůj majetek. Historicky lidé využívali prostředky dostupné z nejbližšího okolí, ze kterých se vytvářely první tzv. mechanické zábranné prostředky, jako byly zprvu např. ploty z větví, na sucho poskládané kamenné zídky. Později ve středověku pak stavby hradů s důmyslnými padacími mosty, vratovými závorami a obrannými valy. Feudální panovníci, ale i obchodníci této doby, vytvářeli pro ochranu svého majetku a pro svoji obranu vycvičené a vyzbrojené soukromé jednotky - fyzickou ochranu. Postupně, poplatně s dobou vznikaly sofistikovanější metody a techniky zajišťující ochranu života a majetku.

S použitím elektřiny přišel rozmach ve vývoji elektrického zabezpečení. Jedním z prvních průkopníků byl v letech 1859 až 1880 Američan Edwin Holmes, který se v městě New York zasloužil o komercializaci elektromagnetického alarmu a o zřízení prvních sítí alarmu proti vloupání. Po druhé světové válce bylo zaevidováno v oblasti elektrické zabezpečovací techniky pro domácí použití mnoho patentů. V druhé polovině 90. let 20. století elektronické zabezpečovací systémy výrazně zlevnily a staly se univerzální, variabilní a dostupné široké veřejnosti. V současné době patří slaboproudé poplachové, tísňové a zabezpečovací systémy společně s kamerovými systémy, mechanickými zábrannými prostředky, elektronickou kontrolou vstupu a dohledovými přijímacími poplachovými centry ke standardům zajišťování ochrany zdraví, života a majetku.

S historickým vývojem zabezpečovací techniky, zejména ve společnostech založených na demokratických principech, začíná vznikat společenská potřeba vytvářet pravidla k používání těchto bezpečnostních technologií. Vznikají tzv. bezpečnostní politiky, technické normy, které používání bezpečnostních, dohledových, obranných a sledovacích technik upravují a formují do zákonných podmínek. Dodržování zákonem stanovená pravidla je tedy možné v demokratické společnosti vymáhat, kontrolovat a sankcionovat. Po vzniku samostatné České republiky rozmach v bezpečnostních politikách nastává před samotným vstupem do NATO, následně pak i do EU.

„Oblast bezpečnosti patří trvale mezi priority lidské společnosti. Ve své podstatě se dotýká všech jejích oborů a úrovní. Fungují-li systémy bezchybně, potřeba bezpečnosti není prioritou. Jiná situace nastane, dojde-li k degradaci nebo úplnému

přerušení funkce. Ihned se volá po její obnově a hledají se způsoby, jak toho dosáhnout. Otázka bezpečnosti se tak stává prioritou. Díky dlouhodobému společenskému vývoji se člověk i společnost stali v této oblasti proaktivní a snaží se na kritické situace dopředu připravit“.[1]

Bezpečnost je proces, nikoliv produkt, ve kterém musí být jednoznačně definována pravidla a rámec odpovědnosti. K tomuto účelu mají sloužit, a to zejména ve státním sektoru , základní standardizované vnitřní předpisy, které by dále měly podléhat bezpečnostním auditům.

Bezpečnost má dvě základní charakteristiky. Objektivní, která se odvíjí od reálně existujících hrozeb a subjektivní, kde stránka bezpečnosti vyplývá z toho, jak konkrétní stát, vnímá dané hrozby, jaký význam jim přisuzuje a jak na ně reaguje.[2]

[1] Lukáš L. a kolektiv*: Bezpečnostní technologie, systémy a management II., 2012,* s. 12.
[2] PORADA, V a kolektiv. *Bezpečnostní vědy. Plzeň: Aleš Čeněk, 2019*, s. 27-28.

1 Cíl a metodika bakalářské práce

Cílem práce je analýza bezpečnostního významu základních vnitřních předpisů pro provozování systémů technické ochrany (dále jen „STO“) objektů v organizacích řízených českým státem. Výstupem a vedlejším cílem bakalářské práce bude návrh základních vnitřních bezpečnostních předpisů, státní organizace a veřejné správy apod. Výsledky této práce by mohly posloužit jako podklad či návod pro zkvalitnění předpisů v této oblasti. V teoretické části bakalářské práce se budu věnovat základním údajům o objektové bezpečnosti a legislativní úpravě STO objektů v ČR. Pokusím se nastínit možný vývoj moderních systémů ochrany objektů v ČR.

V praktické části práce budou shrnuty výsledky empirického šetření formou rozhovorů s odborníky: zástupcem komerční společnosti poskytující specializované služby v oboru, dodavatelem bezpečnostních systémů, pověřencem pro ochranu osobních údajů, bezpečnostním manažerem zdravotní pojišťovny, členy Asociace bezpečnostních manažerů a členy Komory podniků komerční bezpečnosti ČR. Empirické šetření bude zaměřeno na bezpečnostní politiky, na jejich pravidla a zejména na význam vnitřních bezpečnostních předpisů, které definují nastavené standardy bezpečnosti uvnitř organizace a které tak rozhodují o tom, jak jsou jednotlivá aktiva chráněna. Zároveň bude provedeno dotazníkové šetření u vybraných manažerů bezpečnosti v organizacích řízených českým státem, s cílem analyzovat strukturu a rozsah vnitřních předpisů v oblasti bezpečnosti.

Bakalářská práce si klade za úkol upozornit na neexistenci uceleného právního předpisu pro bezpečnostní management, který by standardizoval rámec pro provozování a správu STO objektů v organizacích řízených českým státem. Úkolem bezpečnostního managementu je chránit organizaci v souladu s platnými zákonnými právními akty ČR, sledovat dodržování bezpečnostních směrnic uvnitř organizace, navrhovat jejich aktualizaci a realizovat provedení změn v bezpečnostních politikách. Ucelený rámec vnitřních bezpečnostních předpisů, společně se sjednocenou bezpečnostní terminologií, (jako např.“ výklad základních pojmů[3]), neboli pojmoslovím a definicemi, může pak velkým dílem přispět k částečné standardizaci postupů při tvorbě bezpečnostní

[3] *Česká bezpečnostní terminologie, výklad základních pojmů.* ÚSTAV STRATEGICKÝCH STUDIÍ VOJENSKÉ AKADEMIE V BRNĚ, 2002. [online]. Dostupné z WWW: https://moodle.unob.cz/pluginfile.php/11277/course/section/3043/%C4%8Cesk%C3%A1%20bezpe%C4%8Dnostn%C3%AD%20terminologie.pdf.

dokumentace v organizaci řízené českým státem. O nutnosti zavést určitou jednotnou soustavu alespoň základních pojmů a společnou obecně přijímanou terminologií v oblasti bezpečnosti je v knize *„Bezpečnostní vědy“*[4] popsáno několik kapitol. O problematičnosti a neujasněnosti bezpečnostní terminologie podle DANICS[5] souvisí s následujícími skutečnostmi např. v nejednotném chápání základních pojmů, česká bezpečnostní komunita se utváří a není zatím ustálena, což se mimo jiné projevuje v terminologické roztříštěnosti, která je zřetelná při přípravě českých národních bezpečnostních dokumentů.

[4] PORADA, V a kolektiv. *Bezpečnostní vědy. Plzeň: Aleš Čeněk, 2019*, *1.2 terminologie v oblasti bezpečnosti,* s. 27.
[5] DANICS, Š. *Bezpečnostní politika ve veřejné správě*, s. 7 – 10.

2 Vývoj moderních systémů technické ochrany objektů

Bude-li nás zajímat rychlost rozvoje a pokroku bezpečnostního průmyslu a tím i vývoj bezpečnostních technologií, musíme si nejdříve uvědomit, že k přiblížení se k „bezpečnému prostředí“ se používají různá odvětví průmyslu s různými rychlostmi vývoje konkrétních technologií. Dynamický rozvoj mechanických zábranných prostředků, elektronických zabezpečovacích systémů a kamerových systémů za posledních čtyřicet let, přinesl do oblasti bezpečnostního průmyslu zásadní změny, a to zejména do oblasti technického zabezpečení objektů.

Využívají se nové slitiny materiálů odolných proti mechanickému a tepelnému poškození. Dále vývoj materiálů pohlcující radiové vlny, tj. obrana proti zaměření. Miniaturizace nejen čipů, ale i dalších koncových komponentů, větší životnosti napájecích baterií a sofistikovanější systémy dobíjení. Díky prudkému vývoji digitalizace dochází k úzkému propojení fyzické a informační bezpečnosti. Dnešní moderní systémy umí porovnávat a vyhodnocovat určité fyzikální veličiny, umí se učit a bez zásahu člověka v některých případech i samy konají. V současné době probíhá vlna integrace těchto digitálních systémů a spolupráce mezi nimi, ale i spolupráce s dalšími řídícími centrálními systémy budov (klimatizace, centrální vysávání, udržování vlhkosti a teploty uvnitř objektu apod.).

Vzhledem k rychlému a neustálému technologickému vývoji v oblasti kamerových systémů, již nedochází k posuzování detailních parametrů jednotlivých zařízení. Moderní kamerové systémy jsou popisovány jako celek, který se skládá z více funkčních bloků a vztahů mezi nimi. Základním funkčním blokem je: „videoprostředí“, „management systému“ a „bezpečnost systému“.

Dnešní kamerové systémy již používají biometriku, rozpoznávají teploty objektu, nebezpečného chování objektu, rozpoznání odloženého zavazadla, snímání registračních značek vozidel při vjezdu na parkoviště a při řízení dopravy. Systém identifikace lidských tváří umožňuje rozpoznávat v jednom okamžiku stovky nebo i více detailů. Slouží zejména k vyhledávání podezřelých nebo nebezpečných osob, které jsou předmětem zájmu bezpečnostních služeb. Optika kamery umí pracovat s různými barevnými spektry, které využívají i vesmírné teleskopy nebo družice snímající povrch země s velkým rozlišením např. mapy určené pro navigaci v terénu. Nelze opomenout vývoj sledovací audiovizuální techniky pro potřeby armády a bezpečnostních složek

státu za účelem zajištění jeho bezpečnosti a oprávněných zájmů. Kamerový systém umí automaticky vyhodnotit spoustu veličin, které byly dříve předmětem složité analýzy samotných systémů řízení budov pomocí jednotlivých čidel (přítomnost osob, vytápím, svítím, klimatizuji apod.) Tento trend zvyšuje efektivitu všech investic do řídících a bezpečnostních systémů a zároveň snižuje energetickou náročnost. Je otázkou, kde je hranice a jaká jiná rizika touto integrací mohou vznikat.

Další dynamicky se vyvíjející prostředí je ovládání elektronických systémů pomocí aplikací v mobilních telefonech, kdy lze zabezpečení objektu na dálku vypnout, zapnout nebo odpojit konkrétní koncový prvek, který vykazuje chyby. Kamery umožňují nejen v reálném čase monitorovat zabezpečený prostor, ale i pachatele verbálně vyzvat k jeho opuštění. Do budoucna bude nepochybně docházet nejen ke zlepšování a rozšiřování možností detekce u jednotlivých čidel, a tím k jejich vyšší universálnosti, ale zároveň i k zapojení umělé inteligence řídící spolupráci mezi jednotlivými systémy a komponenty. Tedy k vyšší úrovni automatizace.

V obranném a bezpečnostním průmyslu postupuje mílovými kroky vpřed i robotizace. Roboti určení k zneškodnění nastražených výbušnin, létající drony, bezpilotní letadla s výdrží ve vzduchu až 50 hodin. Vojenské, hasičské nebo důlní speciály ovládané na dálku. Různě složité typy robotů také nahrazují člověka ve výrobních procesech. Vývoj robotiky jistě přinese do oblasti komerční bezpečnosti pokročilé záchranářské roboty asistenty, kteří budou schopni např. monitorovat zdravotní stav, přivolat první pomoc nebo dopravit zraněného na určené místo. Roboti a drony opatření kamerovými systémy napojení na centrální řídicí systém budou jednou chránit celé komplexy obytných budov a výrobních hal, zajišťovat veřejný pořádek v ulicích měst a možná nahradí v mnoha případech městkou i dopravní policii.

Na závěr lze konstatovat, že vývoj informačních a komunikačních technologií (ICT) mění každým rokem svět, a to čím dál dynamičtěji.

3 Systémy technické ochrany objektů

Úkolem mé práce není podrobně popsat jednotlivé STO objektů, ale zaměřím se pouze na základní popis a rozdělení jednotlivých STO objektů.

Co je to ochrana objektů a jaký je cíl a význam STO?

STO objektů je tvořen kombinací jednotlivých druhů bezpečnostních systémů, technologií nebo opatření, které mohou být navzájem propojovány viz „Obr. 1: Systémy a technologie objektové bezpečnosti“. Pod pojmem chráněný objekt si představujeme nejen samotnou budovu, ale zejména materiální vybavení a chráněné informace uvnitř objektu. Cílem a úkolem ochrany objektů je:

a) **odrazovat** od samotného napadení objektu a vzbuzovat dojem, že se nevyplatí riskovat,

b) **zabraňovat** napadení a poškození objektu, co nejvíce ztížit pachateli proniknout,

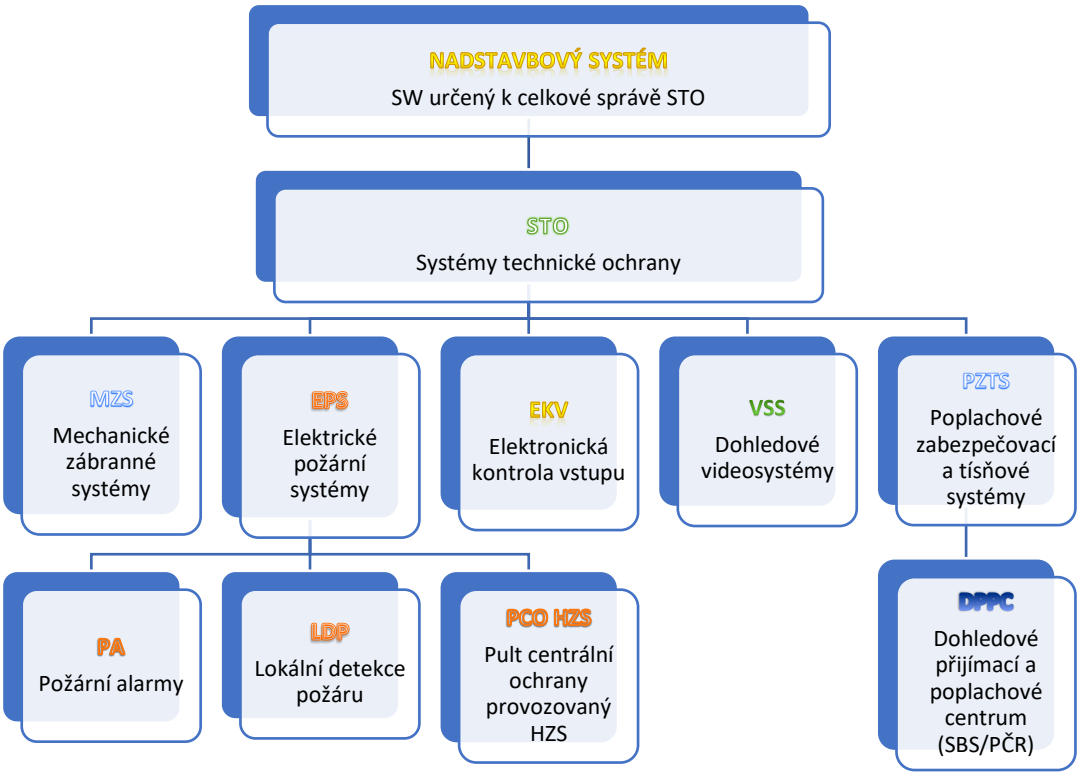
c) **detekovat** napadení chráněného objektu, zaznamenat místo vniknutí a vyhlásit adekvátní poplach,

d) **reagovat** na napadení objektu, okamžitá reakce a zásah fyzické ostrahy, výjezd soukromé bezpečnostní služby (dále jen „SBS“) nebo složek integrovaného záchranného systému (dle jen „IZS“) podle druhu napadení,

e) **provést**, na základě vyhodnocení napadení, nová bezpečnostní opatření.

Před samotným návrhem zabezpečení a instalací STO je nutno provést bezpečnostní klasifikaci, provést analýzu rizik a vypracovat bezpečnostního posouzení objektu (dále jen „BPO“). V BPO neopomenout celou řadu detailů, zdánlivě nepodstatných, ale v souhrnu důležitých, které mohou být spouštěčem selhání celého systému. BPO stanoví způsob, rozsah a stupeň zabezpečení. Definuje mimo jiné bezpečností zóny, zabezpečené oblasti a přístupy k nim. Následuje samotná instalace bezpečnostního systému, zkušební provoz, převzetí díla a poučení obsluhy se samotným provozováním (provozní knihy, údržba systému, pravidelné revize a funkční zkoušky, servis).

Obrázek 1: Systémy a technologie objektové bezpečnosti[6]



K výše vyjmenovaným činnostem ohledně správy STO, je nezbytné mít vnitřním předpisem zpracované postupy a stanovené odpovědnosti. Jedním z důvodu je, že u některých elektronických systémů dochází ke zpracování osobních údajů zaměstnanců např. při používání identifikačních karet (dále jen „ID“) u systémů elektronické kontroly vstupu (dále jen „EKV“). Taktéž kamerové systémy se záznamem dle Úřadu pro ochranu osobních údajů (dále jen „ÚOOÚ“) podléhají pravidlům pro zpracování osobních údajů[7].

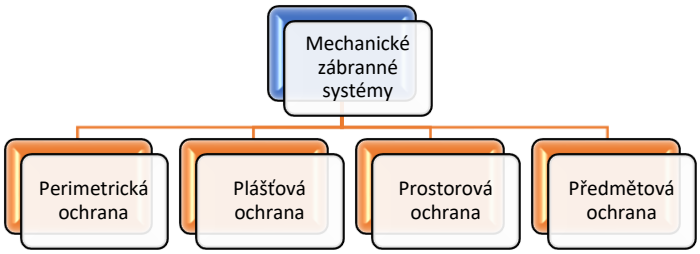
Mechanické zábranné systémy (dále jen „MZS“).

MZS jsou základním pilířem ochrany a z hlediska vývoje patří mezi úplně nejstarší způsob a typ ochrany objektů. K ochraně objektů např. bytů, nebytových prostor, skladů a dále např. výrobních hal, přispívají svojí mechanickou odolností. Mají tzv. zpožďovací faktor. V naší moderní době se MZS již běžně kombinují

[6] „Zpracováno autorem.“. Inspirace podle způsobu správy STO společnosti, ve které je autor zaměstnán.
[7] ÚOOÚ – *K provozování kamerových systémů.* [online]. Dostupné z WWW: https://www.uoou.cz/k-provozovani-kamerovych-systemu/d-29535.

s elektronickými zabezpečovacími systémy, jako jsou elektronické závory, nášlapné a kamerové systémy apod. Jednotlivé MZS řadíme do technické ochrany objektů a rozdělujeme je podle účelu využití do čtyř oblastí, viz „Obr. 2: Rozdělení mechanických zábranných systémů“.

Obrázek 2: Rozdělení mechanických zábranných systémů[8]



Pod MZS si představujeme takové mechanické prvky a komponenty, které po určitou dobu odolávají násilí pachatele. Jsou to např. cylindrické vložky zámků, bezpečnostní kování, opancéřování vstupních dveří s vícebodovým uzamykacím systémem, zárubně s bezpečnostními závěsy, které jsou vylité betonem. U oken pak mříže, bezpečnostní fólie nebo vícevrstvá skla. Pro vstupy a vjezdy, které jsou součástí hranice chráněného prostoru, používáme různé typy bran, závor, turniketů a bezpečnostních propustí, jako jsou např. hřebové bariéry a zastavovací pásy.

Norma ČSN EN 1627 až ČSN EN 1630 určuje požadavky a systém klasifikace vlastností odolnosti proti vloupání u dveří, oken, lehkých obvodových plášťů, mříží a okenic a dalších otvorových výplní včetně jejich komponentů např. zámků a kování, tedy souhrnně MZS. Definuje celkem 6 bezpečnostních tříd, viz „Tab. 1: Bezpečnostní třídy MZS“ se zkratkou RC.

Dobrým pomocníkem při aplikaci MZS je „Sborník technické harmonizace 2013“[9] vydaný Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví (ÚNMZ).

[8] Rozdělení inspirováno podle: HALOUZKA, K. *Fyzická bezpečnost. Téma Perimetrické zabezpečovací systémy* [online]. Dostupné z WWW: https://docplayer.cz/4405209-Fyzicka-bezpecnost-tema-perimetricke-zabezpecovaci-systemy-ing-kamil-halouzka-ph-d-kamil-halouzka-unob-cz.html.
[9] Sborník technické harmonizace [online]. Dostupné z WWW: http://www.azks.cz/data/clanky/files/000140.pdf.

Tabulka 1: Bezpečnostní třídy MZS[10]

Bezpečnostní třída	Předpokládaný způsob napadení
RC1	Příležitostní zloděj se pokouší o vloupání s použitím jednoduchého nářadí a fyzického násilí např. kopáním, narážením ramenem, zdviháním, vytrháváním. Zloděj nemá žádné zvláštní znalosti o úrovni odolnosti MZS, má málo času a snaží se nepůsobit hluk.
RC2	Příležitostní zloděj se navíc pokouší o vloupání za použitím jednoduchého nářadí a fyzickým násilím. Má malé znalosti o úrovni odolnosti MZS, má málo času a snaží se nepůsobit hluk.
RC3	Zloděj se snaží překonat MZS při použití páčidla délky 710 mm a dalších šroubováků, ručního nářadí, jako malé kladívko, důlčíky a mechanická ruční vrtačka. Zloděj má určité podvědomí o systému uzávěru a s tímto nářadím je schopen těchto znalostí využít. Při použití páčidla délky 710 mm lze aplikovat zvýšené fyzické násilí.
RC4	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.
RC5	Velmi zkušený zloděj využívá navíc jednoruční elektrické nářadí např. úhlovou brusku do průměru kotouče 125 mm, přímočarou pilu atd. Neznepokojuje se hlukem.
RC6	Velmi zkušený zloděj používá navíc dvouruční elektrické nářadí např. úhlovou brusku o průměru kotouče 230 mm, přímočarou pili atd. Neznepokojuje se hlukem.

Perimetrická ochrana:

Jedná se o 1. linii ochrany (obvodová ochrana) – o okolí střeženého objektu např. zahrady, dvory, parkoviště nebo skladovací a odkládací plochy. Cílem je zajistit ochranu na vymezené hranici. Tou je zpravidla zeď, plot a vstupy do vymezeného chráněného prostoru, jako je branka, vrata, závora, elektrické ohradníky apod. Smyslem perimetrické ochrany je zaznamenání nepovoleného vstupu narušitelem dříve, než se dostane k chráněnému objektu. U velmi důležitých objektů a k nim přiléhajících velkých volných ploch, jako jsou např. civilní a vojenská letiště, je bezpečnost

[10] KOKTAN, P. *Nové označení bezpečnostních tříd mechanických zábranných systémů není jen prekabatenie* [online]. Dostupné z WWW: https://www.bezpecnostni-dvere-mrize-kavan.cz/wp-content/uploads/2013/03/secmag_1-2013aga-WEB-kopie.png.

perimetru kombinována s kamerovým systémem (dále jen „VSS“), fyzickou ostrahou a dalšími elektronickými bezpečnostními systémy.

Plášťová ochrana:

Jde o 2. linii ochrany (objektová ochrana). Jde o místa, kde lze proniknout do objektu jeho pláštěm např. okna, dveře, mříže, vrata, světlíky, vikýře a šachty. Řeší i méně známé způsoby průniku do objektu, a to samotným pláštěm.

Prostorová ochrana:

3. linie ochrany – chrání vnitřní prostory objektu, které jsou rozděleny na jednotlivé bezpečnostní zóny např. spisovny, datová centra, pokladny, vývojové laboratoře apod. V objektu je využíván tzv. systém generálního klíče. Bezpečnostní zóny zabezpečujeme v kombinaci MZS, poplachové zabezpečovací a tísňové systémy (dále jen „PZTS“), EKV a při vstupech s VSS.

Předmětová ochrana:

4. linie ochrany – řeší zabezpečení konkrétních předmětů. Patří mezi ně především: trezorové místnosti, pokladní časové trezory, úschovné objekty - skříně, trezorové skříně na zbraně a bezpečnostní zavazadla určená k převozu cenin apod. K ochraně historických předmětů v muzeích a při výstavách např.: různými čidly snímající teplotu, pohyb, váhu předmětu apod.

K **předmětové ochraně speciální** používáme různé chemické prostředky např.: prášky, lepidla, pasty, laky, vosky, pudry, zadýmovací zařízení a jiné chemické nástrahy. U mechanických prostředků např.: pečetě, hologramy, kolky, plomby, vodoznaky, zvukové signály.

Poplachové zabezpečovací a tísňové systémy.

PZTS je soubor prvků aktivní, ale i pasivní ochrany, tedy komponentů (ústředna, ovládací klávesnice, detektory) schopných reagovat na narušitele dálkově, ale i místně např. akusticky sirénou nebo vizuálně majákem. Signalizovat a odesílat poplachové stavy o proniknutí nebo pokus o proniknutí do chráněného objektu. PZTS sama o sobě neumí zabránit napadení objektu, ale získává informace z koncových prvků, tj. detekuje a analyzuje momentální stav chráněného prostoru. V případě napadení PZTS informuje v reálném čase fyzickou ostrahu, která je přímo v místě objektu, dálkově na mobilní

telefon majitele nebo na dohledové přijímací a poplachové centrum (dále jen „DPPC“), které provozují soukromé bezpečnostní služby a Policie české republiky (dále jen „PČR“).

PZTS lze instalovat v drátové nebo i v bezdrátové variantě. Bezdrátová varianta je šetrná k budově tzn., že se nemusí kabeláž zasekávat pod omítku, provádět průrazy skrze stěny apod. Je ale limitována dosahem čidel a životností baterií. Koncové prvky jsou u kvalitních a certifikovaných systémů dodávané s vlastní detekcí, která i při odstřežení systému umí vyhodnotit a poslat poplachový stav o svém zničení nebo násilném odpojení, zakrytí nebo o jiném omezení své činnosti. Dále PZTS dělíme i podle výše stupně zabezpečení, to znamená, že celý systém je na úrovni zabezpečení nejslabšího článku. Výrobci komponentů PZTS dnes vyrábí prvky, která certifikují na stupně zabezpečení dle ČSN EN 50131-1.

Tak jako rozdělujeme MZS dle účelu a jeho využití, obdobně rozdělujeme i PZTS, které následně využíváme k:

a) **plášťové ochraně** – detektory otevření vstupů, jako např. dveří a světlíků (magnety), detektory tříštění skla (audio senzory), otřesové detektory (vibrace při řezání, vrtání), nášlapné detektory. K plášťové ochraně se dále využívá kombinace PZTS a VSS,

b) **prostorové ochraně** – doplňuje plášťovou ochranu o prostorové detektory pohybu (např. pasivní infračervený senzor, aktivní ultrazvukový senzor, aktivní mikrovlnný senzor, duální kombinovaný senzor). K prostorové ochraně dále patří kombinace PZTS/EKV s VSS,

c) **předmětové ochraně** – k předmětové ochraně se využívají speciální senzory nebo detekční kabely, které jsou umístěné přímo na chráněném předmětu (např. otřesová čidla na trezorech). Dále se využívají nejrůznější úschovné objekty - úschovné schránky a skříně, domácí a hotelové trezorky, přenosné kontejnery. Podle určení je lze dělit na úschovné objekty bezpečnostní (odolné proti vloupání po určitou časovou jednotku) a na úschovné objekty ohnivzdorné (odolné proti účinku ohně). Podle použití mohou být pevně a skrytě připevněné ke stěně nebo zabudované do zdi.

d) vyvolání **tísňového stavu** – využívají se např. paniková tlačítka, která slouží k rychlému, téměř okamžitému předání tísňové informace na ostrahu objektu nebo na DPPC, či jinému článku bezpečnosti. Jejich využití je ve všech provozech, kde hrozí loupeže nebo nátlak na zaměstnance. Je možno využít široké škály drátových i bezdrátových tlačítek ve formě klíčenky, strhávacích tlačítek atd. Paniková tlačítka jsou součástí instalovaného PZTS.

Stupeň zabezpečení určuje norma ČSN EN 50131-1 ed.2, kde rozlišuje 4. stupně zabezpečení viz „Obr. 3: Úroveň rizika a stupeň zabezpečení“.

Obrázek 3: Úroveň rizika a stupeň zabezpečení[11]

Stupeň zabezpečení		Úroveň bezpečnostního rizika	Základní opatření	Kategorie dle NBÚ
Narušitelé mají malou znalost s PZTS a mají omezený sortiment nástrojů	1	Nízké	Jednoduché mechanické zabezpečení.	Vyhrazeno
Narušitelé mají určité znalosti s PZTS a používají základní nástroje	2	Nízké až střední	Zvýšené MZS, instalace PZTS + DPPC.	Důvěrné a Tajné
Narušitelé dobře znají PZTS a k dispozici mají kompletní sortiment nástrojů	3	Střední až vysoké	Vyšší MZS, instalace PZTS + DPPC, EKV, organizační režimové opatření	
Narušitelé jsou schopni nebo mají zdroje na vypracování podrobného plánu na vniknutí a mají kompletní sortiment nástrojů a zařízení umožňující nahradit prvky PZTS	4	Vysoké	Rozsáhlé STO, napojení na DPPC PČR, organizační režimové opatření + stálá 24 hod. služba zajištěná více osobami – ostraha objektu	Přísně tajné

Elektronická kontrola vstupu:

Systém EKV pro použití v bezpečnostních aplikacích představují jeden z typů poplachových systémů, které je možno definovat jako systémy obsahující konstrukční a organizační opatření a dále zařízení, nutné pro řízení vstupu[12].

EKV neboli také přístupový systém (Power Key), v dnešní době plnohodnotně nahrazuje klasické klíče a systémy generálního klíče. Nahradit a zablokovat ztracenou kartu je mnohem levnější než nahradit klíč, který je součástí systému generálního klíče.

[11] Podle ČSN EN 50131-1 ed.2, dále doplněno autorem o kategorii NBÚ dle vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.
[12] LUKÁŠ, L., a kolektiv. *Bezpečnostní technologie, systémy a management IV.* 1. vydání. Zlín: VeRBuM, 2014, s. 17.

EKV slouží k efektivnímu zamezení vstupu neoprávněných osob do budovy nebo konkrétní místnosti. Po přiložení ID nebo otisku prstu ke čtečce systému kontroly vstupu, systém okamžitě rozpozná, zda do prostoru chce vstoupit oprávněná či neoprávněná osoba. Vstup do zabezpečeného prostoru je následně umožněn pouze oprávněné osobě. Přístupový systém umožňuje nejen řízení pohybu osob, ale i vozidel a jejich sledování v reálném čase s nadstavbovou možností grafického znázornění na mapě chráněného objektu.

Ve většině případů se systém EKV pořizuje společně s PZTS (oba systémy pak využívají jednu ústřednu) nebo samostatně, kdy lze EKV integrovat do již instalované PZTS na objektu. Samostatný systém lze využít v hotelích a nemocnicích. Systém může být doplněn dalšími softwarovými moduly, například objednáváním a výdejem stravy nebo v rámci docházkového systému.

ID karty:

ID karty slouží primárně k identifikaci svého uživatele a k nastavení povolení vstupu do konkrétního prostoru a podle nastaveného oprávnění do jednotlivých chráněných prostor uvnitř objektu. Stejnou kartu lze využít v docházkovém systému nebo při platbě v podnikové jídelně či bufetu.

ID karty jsou moderní identifikační médium. Jsou opatřeny bezkontaktním čipem, který je spojen s měděnou anténkou. Čipy využívají různé frekvence. Vše je zalisované v plastu, v těle karty. ID karty lze libovolně potisknout. Na trhu je k dostání několik druhů ID karet, které lze rozdělit na karty pouze pro čtení ID čipu nebo na karty určené pro čtení a zápis:

a) **karty s čipy určené pouze pro čtení** slouží pro pouhou identifikaci. Využití je především k jednoznačné identifikaci při vstupu (zákaznický, přístupový, hotelový apod.),
b) **karty s čipy určené pro čtení i zápis** umožňují identifikaci, ale především ukládání dat do čipu,
c) **karty s čipy pro čtení i zápis,** lišící se od karty viz písm. b) pouze množstvím dat, které je možné uložit do paměti čipu a způsobem jejich zabezpečení. Tyto karty jsou nejčastěji využívány v dopravě nebo jako elektronická peněženka,

d) **bezkontaktní karty kombinované**, řeší spojení několika identifikačních systémů jedním identifikátorem – kartou, která obsahuje dva čipy pracující na dvou různých frekvencích. Využívá se především u propojených systémů, kde jsou používány čtečky s různými frekvencemi čtení a systémem platebním – elektronická peněženka.

Docházkový a návštěvní systém:

Již nežijeme v době, kdy se příchod na pracoviště evidoval přes vrátnici za pomocí tzv. píchacích hodin nebo zápisem v knize docházky, ale v době digitalizace. Pokročilé systémy čtečky ID karet nepotřebují, jsou postavené v tzv. cloudu[13] a komunikace je online za pomoci přihlašovacích údajů. Docházkový systém umožňuje spravovat pracovní dobu zaměstnanců dislokovaných i z několika poboček (vzdálenost nehraje roly), jejich absence, zadávání a schvalování žádostí (uvolnění pro: návštěva lékaře, svatba, úmrtí v rodině apod.) a upravovat tzv. plovoucí pracovní dobu, práce z domova, přesčasy, týmové rozvrhy a dále např. služební cesty. Systém zbavuje chybovosti při manuálním zpracovávání a přepočítávání nároku na výši mzdy.

Návštěvní elektronický systém slouží k evidenci vstupu a výstupu cizích subjektů do objektu organizace. Systém je součástí režimové ochrany uvnitř objektu. Je buď samostatný, nebo je součástí docházkového systému či EKV. Poskytuje informace o tom, kolik osob je v objektu, kdo byl navštíven a jak dlouho.

Obchůzkový systém:

V rámci plášťové a prostorové ochrany objektů je využíván obchůzkový systém. Slouží pro kontrolu a evidenci obchůzkové činnosti strážných z SBS. Základem systému je elektronické čtecí zařízení, kterým se osoba provádějící obchůzku identifikuje na kontrolních bodech. Některé systémy pracují v reálném čase, kdy snímače komunikují přímo s dispečinkem DPPC. Ve střeženém prostoru jsou rozmístěny na kontrolních bodech snímače, které musí strážný v daném pořadí a čase obejít se čtecím zařízením, je tak přesný přehled o tom, zda je objekt střežen dle smluveného postupu.

[13] Cloud, termín, který se používá pro popis globální sítě serverů, z nichž každý má svoji funkci. Cloud - *česky* ***mrak*** – kreslit ve schematických obrázcích komunikace.

Dohledové videosystémy:

Kamerové systémy jsou nedílnou součástí bezpečnosti objektů skoro osmdesát let. Původně se nazývaly „průmyslová televize“ (PTV), později jako „uzavřený televizní okruh“ (CCTV). Nově se kamerové systémy nazývají „dohledové videosystémy“ (VSS) a jsou díky své dynamice vývoje vysoce účinným bezpečnostním prvkem. Na základě požadavku uživatele, slouží kamerové systémy zejména pro identifikaci, detekci, rekognici a monitorování zájmových částí.

Kamerový systém se skládá z kamer, úložiště, monitorovacího zařízení pro účely přenosu obrazu, ovládání, ukládání záznamu a jeho dalšího zpracování. Pomocí vhodně rozmístěných kamer lze úspěšně monitorovat prakticky veškeré dění v okolí, ale i uvnitř chráněného prostoru.

Kamerové systémy pro potřebu ochrany objektů umožňují:

- monitorování vybrané scény např. bezpečnostní a přehledové funkce, a to i za snížených viditelných podmínek,
- perimetrickou ochranu střeženého prostoru,
- rozpoznání obličeje – umožnění vstupu do objektu a vybraných chráněných prostor (datové sály, archivy, vývojové a konstrukční kanceláře apod.)
- rozpoznávání registračních značek motorových vozidel – automatické vjezdy a výjezdy (ovládání závor, vrat do podzemních garáží, autovýtahů apod.),
- registrace a upozornění na odložené předměty,
- počítání osob.

Nejčastěji se využívají IP[14] kamery, které se nachází na světovém trhu přibližně 10 let a od začátku procházejí dosti významnou evolucí. Především co se týče různorodosti jejich konstrukčního provedení. IP kameru lze uvádět také jako síťovou kameru, jednoduše lze říci, že se jedná o kombinaci kamery a počítače. Moderní IP kamerové systémy založené na digitální technologii lze propojit za pomoci nadstavbového softwarového systému s PZTS i EKV. V některých případech část těchto systémů již samotné IP kamery nahrazují, a to vestavěnými čidly s konkrétním účelem zaměření a smyslem využití.

[14] Internet Protocol (základní protokol používaný v počítačových sítích a internetu).

Před samotným návrhem bezpečnostního kamerového systému je nutno ověřit dostatečnou propustnost počítačové sítě. Pro rozsáhlé systémy s více jak padesáti kamerami, je nutné počítačovou síť pro IP kamery dimenzovat na vyšší přenosovou rychlost, přibližně 1 GB/s[15]. Tímto bude zaručena dostatečná přenosová rychlost, a to i s ohledem na případné rozšíření kamerového systému. Snímaný obraz je zpracováván již přímo v kameře a jeho digitální formát je přenášen do záznamového zařízení. Díky vysokému rozlišení IP kamer jsme schopni vidět mnoho detailů a celková plocha pokrytá jedinou kamerou je pro monitoring střeženého prostoru více jak významná. Záznam z kamery je možné přenášet na libovolnou vzdálenost a ovládání kamer lze řídit na dálku.

Dohledové přijímací a poplachové centrum:

V důsledku neustálé rostoucí kriminality vyvstává obecně stále větší potřeba chránit své zdraví, život i majetek lidí. Tato nutnost vedla již v minulosti k vývoji a instalování takových bezpečnostních zařízení, která by umožnila včasné hlášení poplachových (havarijních) situací ze vzdálených objektů do centrálního dispečinku pro střežení[16]. DPPC přijímají, zpracovávají informace a iniciují odpovídající odezvy a následný zásah na základě informací zprostředkovaných vzdálenými detekčními a monitorovacími systémy[17]. Moderní DPPC nepřijímá jenom stavové hlášky z PZTS, VSS a EKV ale i ze systémů přivolání pomoci[18].

DPPC viz „Obr. 4: Dohledové, přijímací a poplachové centrum“ zajišťují nepřetržitou službu, dohled nad stavy a událostmi střeženého objektu, kdy stavové hlášení ze STO přicházejí po různých komunikačních kanálech, jako jsou např. telefonní linky ISDN[19], po síti GSM[20] v hovorovém pásmu včetně SMS nebo prostřednictvím GPRS[21] a v neposlední řadě pomocí internetové sítě. Operátor DPPC po přijetí poplachu vysílá zásahovou jednotku, která na místě prověřuje stav události. V případě vloupání usiluje o zadržení pachatele, informuje PČR a vyrozumí majitele objektu a v případě pomoci v nouzi poskytuje první pomoc a přivolává RZP[22]. Je-li vyhlášen požární poplach z autonomní detekce a signalizace např. kouřových čidel

[15] Bit za sekundu je jednotka přenosové rychlosti. Udává, kolik bitů informace je přeneseno za 1 sekundu.
[16] KYNCL, J., a kolektiv. *Bezpečnost objektu ve světle moderních technologií*, s. 179.
[17] KAMENÍK, J., BRABEC, F., a kolektiv. *Komerční bezpečnost.* 2. vydání, s. 107 – 108.
[18] ČSN EN 50134-3-ed.2.
[19] Integrated Services Digital Network (digitální síť internetových služeb).
[20] Group Spécial Mobile (buňková síť, mob. tel. se se připojují do sítě prostřednictvím nejbližší buňky.
[21] General Packet Radio Service (umožňuje mob. tel. přenost dat a připojení k internetu.
[22] Rychlá záchranná pomoc - typ výjezdové skupiny zdravotnické záchranné služby.

(objekt není vybaven elektrickou požární signalizací, dále je „EPS“), zásahová jednotka prověří situaci v místě a vyrozumívá majitele objektu a v případě zjištění kouře nebo požáru neprodleně informuje Hasičský záchranný sbor ČR (dále jen „HZS“).

Obrázek 4: Dohledové, přijímací a poplachové centrum[23]

Systémová integrace bezpečnostních technologií:

Jedná se o nadstavbový integrační systém pro správu a řízení bezpečnostních, ale i jiných technologií v objektu nebo areálu, který dále integruje jednotlivé softwary od různých bezpečnostních a slaboproudých zařízení do přehledového a kompaktního celku viz znázornění integrace systémů na „Obr. 5: Systémová integrace bezpečnostních technologií“. Uživateli usnadňuje přehled z jednoho místa a tím umožňuje snadné ovládání jednotlivých systémů. Graficky umožňuje sledovat např. prostupy do objektu, přijímat poplachy a vzdáleně na ně reagovat.

Je-li systémová integrace dobře navržena a realizována, přináší výraznou přidanou hodnotu a snížení provozní režie např. zvýšení bezpečnosti objektů, zkrácení reakční doby na podněty, kontrola oprávnění vstupu a výstupu do zabezpečených oblastí, snadnou analýzu bezpečnostních událostí a reakci na ně, jednotné ovládání integrovaných technologií, grafické znázornění a lokalizaci bezpečnostní události.

[23] https://www.tram-bus.cz/dpp-ma-modernejsi-dohledove-a-poplachove-prijimaci-centrum/.

Samozřejmostí je podpora zařízení s webovým rozhraním. Na druhou stranu zvyšuje závislost na externím dodavateli.

Obrázek 5: Systémová integrace bezpečnostních technologií[24]

Elektrická požární signalizace:

Požární ochrana se týká všech oblastí lidské činnosti. Jak uvádí dále KYNCL[25], požadavky týkající se zajištění požární ochrany diagonálně se prolínají celým spektrem právních předpisů, technických specifikací a jiných regulativ. Synergie požárů, objektů a osob pak vytváří široké spektrum možných variant požárních scénářů. Proto je třeba vytvářet podmínky pro zajištění požární ochrany a požární bezpečnosti již ve fázi územní, předprojektové a projektové přípravy staveb.

Požáry každoročně způsobují nemalé ztráty na životech, zdraví a majetku. Na území ČR při nich zahyne každoročně přes 100 osob a stovky osob jsou zraněny. Přímé škody způsobené požáry dosahují řádu miliard korun. Jedním z opatření pro zvýšení požární bezpečnosti staveb, a tím i ke snížení negativních dopadů požáru, je používání požárně bezpečnostních zařízení[26].

[24] http://www.integoo.cz/produkty-v2/integra-v2.html.
[25] KYNCL, J., a kolektiv. *Bezpečnost objektu ve světle moderních technologií.* Praha: KPKB ČR, 2014, s. 129.
[26] LUKÁŠ, L., a kolektiv. *Bezpečnostní technologie, systémy a management III.* 1. vydání. Zlín: VeRBuM, 2013, s. 108.

Systém EPS představuje soubor komponentů (hlásičů požáru), ústředen, přenosných a jiných doplňkových zařízení viz PZTS, které v souhrnu tvoří samostatný ucelený systém signalizující v místě opticky nebo zvukově požární poplach. Dále přenáší ze systému EPS nebo datové sítě včasnou signalizaci požáru na PCO HZS ČR. V souladu s požárně bezpečnostním řešením (PBŘ[27]) mohou systémy EPS navazovat na funkce dalších technologií v budově, např. výtahy, otevírání požárních klapek, odvětrávání, otevírání dveří únikových východů, využití hlasové výstrahy z reproduktorů nebo o evakuaci budovy.

Systém EPS podléhá pravidelným zákonným kontrolám:

- 1 x za měsíc funkční zkoušky činnosti ústředen a dalších navazujících zařízení,
- 1 x za 6 měsíců funkční zkoušky samočinných hlásičů požáru a zařízení, které EPS ovládá,
- 1 x za rok revize elektrického zařízení.

Základní funkce ústředny EPS:

- monitoring všech instalovaných prvků na poplachových smyčkách systému
- vyhodnocování signalizace prvků a požáru,
- stav kompletního systému (provoz, porucha, požár).

Signalizace poplachu:

- spuštěním sirén, evakuačního rozhlasu – nouzového zvukového systému (NZS),
- stroboskopickým majákem
- využitím firemních IP telefonů, zasíláním SMS zpráv.

Je třeba poznamenat, že za systém EPS nelze považovat autonomní detekci a signalizaci, a to ani čidla detekce kouře nebo podobná čidla (teploty, CO2, plynu), které se instalují v rámci PZTS.

[27] PBŘ stavby se zpracovává na základě § 41 vyhlášky č. 246/2001 Sb. o požární prevenci.

Základní dokumentace k objektové bezpečnosti:

Základní dokumenty (předpisy) k objektové bezpečnosti definují rizika, postupy a pravidla při řízení procesů s cílem zajistit efektivní a jednotnou správu fyzické a technické bezpečnosti. Upřesňují rámec odpovědnosti a další funkcionality systému provozní bezpečnosti.

Přehled dokumentace:

a) analýza rizik je vytvoření analýzy hrozeb a zranitelností a stanovení dopadů a jejich pravděpodobnosti na chráněná aktiva viz „Obr. 6: Znázornění analýzy rizik“. Podle KRULIŠ[28], poskytuje analýza rizik nenahraditelné podklady pro včasnou a efektivní prevenci nežádoucích událostí,
b) bezpečnostní posouzení objektu (dále jen „BPO“) viz „Obr. 7: Schéma bezpečnostního posouzení objektu“, spočívá zejména v získání informací potřebných pro vytvoření návrhu STO, Definuje současný stav objektu a určuje hodnoty aktiv a jejich význam. Určuje a posuzuje vlivy, které působí na STO,

Obrázek 6: Znázornění analýzy rizik[29]

[28] KRULIŠ, J., *Jak vítězit nad riziky. Aktivní management rizik – nástroj řízení úspěšných firem.* Praha: Linde Praha a.s., 2011, s. 391
[29] https://www.cleverandsmart.cz/analyza-rizik-jemny-uvod-do-analyzy-rizik/.

c) bezpečnostní projekt ochrany objektu, obsahuje zejména návrh umístění zabezpečených oblastí v objektu včetně jejich třídy a kategorie. Způsob použití bezpečnostních opatření při vnější a vnitřní ochraně objektu,
d) technická dokumentace objektové bezpečnosti (projekt skutečného provedení), obsahující technické údaje, pokyny a pravidla pro používání technických prostředků, půdorysy s rozmístěním komponentů daného systému v objektu. Knihy provozu, platné revize a funkční zkoušky od každého jednotlivého systému (PZTS, VSS, EKV, EPS),
e) provozní řád, stanovující zejména režim pohybu osob a dopravních prostředků v objektu, režim manipulace s klíči a pravidla pro výkon fyzické ostrahy objektu, obsahující režim vstupu a výstupu osob a vjezdu a výjezdu dopravních prostředků z objektu, a další pokyny pro činnost fyzické ostrahy objektu,
f) režimová opatření, která obsahují pokyny pro ochranu života, zdraví a majetku při vzniku mimořádné situace.

Obrázek 7: Schéma bezpečnostního posouzení objektu[30]

Fyzická ostraha – SBS:

Po pádu železné opony (v roce 1998) byl v ČR, ale i v ostatních zemích východní Evropy zaznamenán okamžitý vzestup a rozmach bezpečnostních služeb. Kromě investic a vlastního know how, které do této části světa přinesly nadnárodní firmy, začaly díky (v České republice přes některé legislativní pokusy stále

[30] https://is.muni.cz/el/fss/jaro2020/BSSb1195/um/Teorie_objektove_bezpecnosti.pdf?lang=en.

přetrvávajícímu právnímu vakuu) vnikat stovky firem zabývajících se všemi možnými druhy bezpečnostních činností. V ostatních zemích EU je činnost SBS regulována buď specifickým zákonem (Slovensko, Belgie, Velká Británie atd.), nebo zvláštní kapitolou živnostenského zákona (Německo)[31].

V podvědomí veřejnosti je pracovník soukromé bezpečnostní služby vnímán jako člověk v důchodovém věku, který si přivydělává tím, že sedí na vrátnici a zdvihá závory, nebo jako ten, který neprošel psychologickými testy u PČR nebo Městské policie. Přitom je tato práce velmi potřebná a žádaná, a pokud jsou na zaměstnance bezpečnostních služeb kladeny požadované nároky, i vysoce prestižní. Profese pracovníka SBS bývá na spodním žebříčku společnosti, mzda se pohybuje v nejnižších tarifních třídách, s nejnižšími nároky na vzdělání, praxi, psychologickém profilu, jazykových znalostí apod. Chybou u organizací řízených českým státem je, že v rámci veřejných zakázek na tyto služby, je jediným a hlavním kritériem nejnižší nabídková cena.

4 Legislativní úprava STO objektů v ČR

Bezpečnostní systém:

Na rozdíl od integrovaného záchranného sytému, který je považován za jednu z nejpodstatnějších součástí českého bezpečnostního systému, nemá bezpečnostní systém státu jako celek dosud jasně vymezenou a legislativně ukotvenou definici. Její absence se pochopitelně promítá do problémů s koordinovanou výstavbou a řízením bezpečnostního systému: je obtížné řídit a budovat něco, co sice de facto existuje, ale zároveň není přesně vymezeno a pojmenováno[32].

Česká republika je jednou z posledních zemí EU, v nichž není dostatečným způsobem upravena problematika komerční bezpečnosti a ochrany majetku[33]. K fyzické bezpečnosti je v ČR vydána desítka zákonů a vyhlášek. Např. zvláštními zákony je ošetřena ochrana utajovaných informací a ochrana osobních údajů, bezpečnost a ochrana zdraví při práci (BOZP) a požární ochrana (PO), krizové řízení a prevence

[31] BALABÁN, M., STEJSKAL, L. *Kapitoly o bezpečnosti.* Praha: Karolinum, 2019, s. 292-293.
[32] BALABÁN, M., PERNICA, B. *Bezpečnostní systémy ČR: problémy a výzvy.* Praha: Karolinum, 2015, s. 9.
[33] FRYŠAR, M. a kolektiv. *Bezpečnost pro manažery, podnikatele a politiky. Praha: Public History Praha. 2006,* s. 10.

závažných havárií. IZS má jasnou právní úpravu. V legislativě je technická ochrana majetku řešena pouze rámcově, tedy v obecné rovině.

Doposud při navrhování rozsahu zabezpečení, samotné realizaci a provozování STO objektů, vycházíme z harmonizovaných technických norem, jejichž využívání je založeno na dobrovolnosti. Technické normy tvoří hlavní soubor zásad a postupů, dle kterých lze v určité kvalitě provozovat konkrétní, jednotlivý systém ochrany objektu. V evropských zemích je bezpečnostní zabezpečovací technika pod působností evropských směrnic. Česká republika je od roku 2004 členskou zemí Evropské unie, proto jsou technické směrnice přejímány vládou České republiky.

Prameny práva:

Nejdůležitější základní legislativa je tvořena zákonem č. 1/1993 Sb., **Ústava České republiky**, která definuje základní práva občanů ČR a zákonem č. 2/1993 Sb., **Listina základních práv a svobod**, která definuje např. právo vlastnit majetek, nedotknutelnost obydlí apod.

Základní výčet pramenů práv v oblasti ochrany života, zdraví a majetku:

- Zákon č. 40/2009 Sb., **Zákon trestní zákoník**. Chrání majetek, zdraví i život osoby. Případného pachatele má od porušení této ochrany odradit. K ochraně osob a majetku se vztahují zejména § 28 nutná obrana, § 29 krajní nouze a § 32 oprávnění použití zbraně.

- Zákon č. 141/1961 Sb., **Zákon o trestním řízení soudním** ve znění pozdějších změn a doplňků (trestní řád). Upravuje postup orgánů činných v trestním řízení tak, aby trestné činy byly náležitě zjištěny a jejich pachatelé dle zákona potrestáni. V § 76 odst. 2 zadržení osoby podezřelé je uvedeno, že osobu přistiženou při trestném činu nebo bezprostředně poté, může omezit kdokoli např. strážný bezpečnostní agentury (fyzická ostraha objektu).

- Zákon č. 89/2012 Sb., **Zákon občanský zákoník**. Upravuje osobní stav osob a soukromá práva a povinnosti osobní a majetkové povahy. Věnuje se ochraně vlastnictví i nedovolenému zásahu.

- Zákon č. 33/2020 Sb., **Zákon**, kterým se mění zákon č. 90/2012 Sb., **o obchodních společnostech a družstvech** (zákon o obchodních korporacích), ve znění zákona č. 458/2016 Sb., a dalších souvisejících zákonů. Věnuje se především úpravě obchodních společností.

- Zákon č. 455/1991 Sb., **Zákon o živnostenském podnikání** (živnostenský zákon). Upravuje činnost např. SBS. Definuje pro SBS požadavky na vzdělání a odbornou způsobilost spojenou s ochranou a ostrahou majetku, osob, přepravou cenin a dále např. provozování DPPC.

- Zákon č. 262/2006 Sb., **Zákon zákoník práce**. Upravuje pracovněprávní vztahy mezi zaměstnancem a zaměstnavatelem.

- Zákon č. 240/2000 Sb., **Zákon o krizovém řízení** a o změně některých zákonů (krizový zákon). Řídí činnost orgánů krizového řízení zaměřených na analýzu a vyhodnocení bezpečnostních rizik a plánovaní, organizování, realizaci a kontrolu činností prováděných v souvislosti s přípravou na krizové situace a jejich řešení nebo ochranou kritické infrastruktury. Do kritické infrastruktury (KI) jsou zahrnuty objekty např. jaderných elektráren, státních hmotných rezerv, vodárenských objektů apod.

- Zákon č. 412/2005 Sb., **Zákon o ochraně utajovaných informací a bezpečnostní způsobilosti**. Upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu, zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy.

- Zákon č. 110/2019 Sb., **Zákon o zpracování osobních údajů**. Zpracovává příslušné předpisy Evropské unie, zároveň navazuje na přímo použitelný předpis Evropské unie[34] a k naplnění práva každého na ochranu soukromí upravuje práva při zpracování osobních údajů.

- Zákon č. 133/1985 Sb., **Zákon České národní rady o požární ochraně**. Účelem zákona je vytvořit podmínky pro účinnou ochranu života a zdraví

[34] Nařízení Evropského parlamentu a Rady (EU) ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

občanů a majetku před požáry a pro poskytování pomoci při živelných pohromách a jiných mimořádných událostech stanovením povinností ministerstev a jiných správních úřadů, právnických a fyzických osob, postavení a působnosti orgánů státní správy a samosprávy na úseku požární ochrany, jakož i postavení a povinností jednotek požární ochrany.

- Vyhláška č. 225/2015 Sb., **Vyhláška o stanovení rozsahu bezpečnostního opatření fyzické ochrany objektů zařazených do skupiny A nebo B**. V § 1 úvodního ustanovení, vyhláška upravuje požadavky na rozsah analýzy možností neoprávněných činností a provedení útoku na objekt, kategorie a povaha režimových opatření, požadavky na zajištění fyzické ostrahy, kategorie technických prostředků a jejich vymezení a způsob rozsahu bezpečnostních opatření přijímaných v objektu.

- Vyhlášky č. 528/2005 Sb., **o fyzické bezpečnosti a certifikaci technických prostředků**. Tato vyhláška stanoví bodové ohodnocení jednotlivých opatření fyzické bezpečnosti, nejnižší míru zabezpečení zabezpečené oblasti a jednací oblasti, základní metodu hodnocení rizik, další požadavky na opatření fyzické bezpečnosti a náležitosti certifikace technického prostředku.

- Vyhláška č. 246/2001 Sb., **Vyhláška Ministerstva vnitra o stanovení podmínek požární bezpečnosti a výkonu požárního dozoru (vyhláška o požární prevenci)**. Stanovuje podmínky požární bezpečnosti u právnických a fyzických osob. Definuje základní požadavky na vybavení prostor právnických a podnikajících fyzických osob věcnými prostředky požární ochrany a požárně bezpečnostními zařízeními.

Technické normy v oblasti bezpečnosti objektů:

Úřad pro technickou normalizaci, metrologii a státní zkušebnictví (ÚNMZ) je organizační složkou Ministerstva průmyslu a obchodu ČR (MPO ČR).

Základní výčet ČSN-EN, který se zabývá ochranou objektů:

- ČSN EN 1627 Dveře, okna, lehké obvodové pláště, mříže a okenice - Odolnost proti vloupání – Požadavky a kvalifikace

- ČSN EN 1630 Dveře, okna, lehké obvodové pláště, mříže a okenice - Odolnost proti vloupání – Zkušební metoda pro stanovení odolnosti proti manuálním pokusům o vloupání,

- ČSN EN 356 Sklo ve stavebnictví - Bezpečnostní zasklení – Zkoušení a klasifikace odolnosti proti ručně vedenému útoku,

- ČSN EN 50 131 – 1 ed. 2 Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 1: Systémové požadavky. Tato ČSN EN 50 131 je součástí souboru norem a technických specifikací. Má dalších několik částí např.: Pokyny pro aplikace, požadavky na odolnost komponentů, metody zkoušek vlivu prostředí, napájecí zdroje, požadavky na zařízení využívající bezdrátové připojení a další, výstražná zařízení, detektory vniknutí apod.,

- ČSN EN 50 136 Poplachové systémy – Poplachové přenosové systémy a zařízení,

- ČSN EN 62676-1-1 Dohledové videosystémy pro použití v bezpečnostních aplikacích. Soubor norem IEC 62676 pro dohledové videosystémy je rozdělen do 4 samostatných částí: Systémové požadavky, Video přenosové protokoly, Analogové a digitální video rozhraní a pokyny pro aplikace, která bude teprve vydána,

- ČSN EN 50518 Dohledová a poplachová přijímací centra. Norma uvádí minimální požadavky na monitorování, příjem a zpracování poplachových zpráv generovaných poplachovými systémy jako součást celkového řešení požáru, bezpečnosti a zabezpečení,

- ČSN EN 60839-11-1 Poplachové a elektronické bezpečnostní systémy – Část 11-1: Elektronické systémy kontroly vstupu – Požadavky na systém a komponenty. Část 11-2 obsahuje pokyny pro aplikace,

- ČSN 34 2710 Elektrická požární signalizace – Projektování, montáž, užívání, provoz, kontrola, servis a údržba. Základní filosofií této normy je dosažení jednotné struktury předpisu pro projektovou přípravu, navrhování, montáž, uvedení do provozu, kontrolu, užívání a údržbu systémů EPS platného v celé

Evropě. Celkem s touto normou souvisí dalších 21 ČSN, 6 zákonů, 10 vyhlášek a 4 Nařízení vlády.

5 Bezpečnostní politika a její význam

Bezpečnost ČR je založena na principu zajištění bezpečnosti jednotlivce, ochrany jeho života, zdraví a majetku. K tomu je nutno zajišťovat bezpečnost státních institucí a rozvíjet procesy a nástroje sloužící k posilování bezpečnosti a ochrany obyvatelstva. To předpokládá i aktivní spolupráce občanů ČR, právnických a podnikajících fyzických osob a orgánů veřejné správy[35].

Bezpečnostní politika je nejdůležitějším dokumentem organizace. Bezpečnostní politika stanovuje postupy, dle kterých se organizace řídí, při plánování ochrany aktiv. Jsou to tedy hlavně pravidla, směrnice a praktiky, které rozhodují o tom, jak jsou aktiva včetně citlivých informací spravovány a chráněny. Bezpečnostní politika jako norma není nikdy finální, a proto by se měla provádět pravidelná aktualizace a to na základě např. bezpečností události, incidentu nebo zhoršené bezpečností situaci v místě. K zásadním změnám tohoto dokumentu by ale nemělo docházet příliš často, a to z důvodu obsahu normy, jejího obecného charakteru.

Bezpečnostní politika často uvádí i základní principy bezpečnosti organizace a formy, jakými bude své představy o bezpečnosti realizovat. Bezpečnostní politika oslovuje zaměstnance organizace, pro které je ve svých obecných principech závazná[36].

V základním obsahu bezpečnostní politiky by měly být zodpovězeny i základní otázky jako např.:

a) kdo je odpovědný za naplnění bezpečnostní politiky stanové managementem organizace,

b) jakým způsobem bude naplňování a následné dodržování bezpečnostní politiky kontrolováno, vynucováno a sankcionováno,

c) jaký je časový plán pro naplňování a uvádění do praxe stanovených cílů v bezpečnostní politice.

[35] VILÁŠEK, J., FUS, J. *Krizové řízení v ČR na počátku 21. Století*. s. 13.
[36] KAMENÍK, J., BRABEC, F., a kolektiv. *Komerční bezpečnost.* 2. vydání. s. 174.

Vnitřní bezpečnostní předpisy jsou důležitým interním aktem řízení. Bez ohledu na konkrétní oblast je nutné, aby vnitřní bezpečností předpisy splňovaly principy systémového řízení. Předpisy musí být dále zpracovávány tak, aby odpovídaly požadavkům právních předpisů ČR a technickým normám ČR a EU.

Časté chyby v bezpečnosti:

a) Absence bezpečnostní politiky a navazujících vnitřních předpisů,

b) neexistence, neaktuálnost nebo nedodržování analýzy rizik,

c) neadekvátní závislost na jednom dodavateli nebo špatný výběr dodavatele,

d) nedostatečné financování bezpečnosti,

e) nízká podpora vedení organizace,

f) stav bezpečnosti se neprověřuje, nepodléhá ani vnitřní auditní kontrole.

6 Bezpečnostní analýza rizik

Zložitosť procesu posudzovania rizík naznačuje množstvo odbornej literatúry, ktorá sa touto problematikou zaoberá. Je možné konštatovať, že neexistuje oblast ľudskej činnosti, ktorá by nevytvárela riziká alebo nebola im vystavená. Výnimkou nie je ani oblast bezpečnosti z pohľadu ochrany objektov, osob, majetku a informácií[37].

Bezpečnostní analýza v sobě zahrnuje formulaci problému (jaké hodnoty chci chránit), sběr dat a třídění informací – bezpečnostní přehled, vlastní bezpečnostní analýzu získaných poznatků a případně i pokus o bezpečnostní prognózu. Návrh alternativních bezpečnostních plánů představuje syntézu poznatků bezpečnostní analýzy a znalostí (ověřených poznatků) možných struktur ochrany objektů, především mechanické ochrany a elektronických kontrolních bezpečnostních systémů[38].

[37] LOVEČEK, T., REITŠPÍS, J. *Projektovanie a hodnotenie systémov ochrany objektov*. SK. Žilina: EDIS, 2011, s. 187.
[38] PORADA, V., a kolektiv. *Bezpečnostní vědy*. Plzeň: Aleš Čeněk, 2019, s. 227.

Vyhodnocení rizik se provádí:

a) Identifikací a popisem druhů a zjištěním množství hrozeb, které by se mohly vázat na chráněný objekt. Jaký majetek a chráněné informace se v objektu vyskytují nebo budou vyskytovat, zejména z hlediska následku neoprávněného nakládání s chráněnými informacemi,

b) popisem a vyhodnocením zranitelnosti vnitřní a vnější ochrany objektu vůči těmto hrozbám,

c) stanovením míry rizika, jako "malé", "střední" nebo "velké", na základě vyhodnocení hrozeb a zranitelnosti objektu,

d) vyhodnocení stavu bezpečnostních opatření a posouzení, zda jejich realizace pro danou míru rizika odpovídá stanoveným bezpečnostním standardům,

e) další vhodná bezpečnostní a režimová opatření, pokud je stav bezpečnostních opatření podle odstavce výše nedostatečný,

f) zjištění rizik, která přetrvávají i po aplikaci bezpečnostních opatření.

7 Bezpečnostní management

Úkolem bezpečnostního managementu je sledovat dodržování stanovených bezpečnostních opatření a to ve všech oblastech bezpečnosti organizace. Navrhuje případné změny bezpečnostní politiky, řeší bezpečnostní události a incidenty, koordinuje školení zaměstnanců v oblasti bezpečnosti. Je garantem ochrany osobních údajů zaměstnanců a vnitřních bezpečnostních předpisů. Spravuje bezpečnostní dokumentaci a registry rizik. Bezpečnostní management má dále za úkol nalézat případné slabiny v bezpečnosti organizace a na nalezené nedostatky navrhovat taková opatření, která by rizika eliminovala na nejnižší možné riziko. Jedním z takových opatření může být i případné doplnění bezpečnostních směrnic společnosti. Management bezpečnosti definujeme dále jako proces:

a) Plánování, které zahrnuje stanovení cílů v bezpečnostní politice a prostředků k jejich dosažení,

b) personální bezpečnosti, tj. obsazování pozic v organizační struktuře těmi nejschopnějšími lidmi, kteří mají v oblasti bezpečnosti zkušenosti a vzdělání,

c) vedení lidí, což znamená, že vedoucí oddělení mají schopnost koordinovat lidské zdroje, vést, usměrňovat, motivovat a stimulovat je,

d) kontrolní činnosti, která zajišťuje skutečný stav bezpečnosti, porovnává ho s plánovaným cílem bezpečnostní politiky.

Důležité je, aby funkce manažera bezpečnosti, byla zařazena do úrovně vrcholového managementu, a to z důvodu zajištění systémového řízení bezpečnosti v organizaci.

8 Empirické šetření

Stanovení a cíl výzkumného šetření:

1) V praktické části budou shrnuty výsledky rozhovorů s odborníky.
2) Zároveň bude provedeno dotazníkové šetření u vybraných manažerů bezpečnosti.

Hlavní hypotéza: V ČR není dostatečně upravena legislativa pro provoz STO.

Vedlejší hypotéza: Potvrdit nebo vyvrátit nutnost standardizovat (nejen bezpečnostní terminologii) základní bezpečnostní předpisy právním aktem, které by vydala poslanecká sněmovna pro organizace, které mají státní spoluúčast nebo jsou přímo řízeny státem. Byl by závazný a podléhal by tak bezpečnostnímu auditu.

Rozhovory:

Mým sledovaným cílem, je při expertních rozhovorech získat informace od respondentů z oblasti bezpečnosti, kteří se danou problematikou dlouhodobě zabývají. Jedná se o osoby, které jsou nositeli kvalifikované a odborné informace a mají v daném oboru nejen teoretické znalosti, ale i praktické zkušenosti. Akademická kvalifikace respondentů nebyla vyžadována.

Připravené otázky se týkají nejvíce problematiky legislativy v oblasti komerční bezpečnosti, tj. ochrany osob a majetku za použití systémů technické ochrany. Dále obsahu a rozsahu vnitřních bezpečnostních předpisů a politik v organizacích řízených českým státem.

Rozhovor trval s jednotlivými respondenty přibližně 30 minut, a to prostřednictvím komunikační aplikace Microsoft Teams. Po představení autora bakalářské práce byla respondentovi objasněna podstata šetření. Následovala uzavřená výčtová otázka za otázkou dle připraveného dotazníku, kdy autor - tazatel označil odpověď respondenta v dotazníku. Uzavřené výčtové otázky jsou uvedeny v příloze č. 1.

Analýza rozhovorů:

Výčtové otázky jsou s respondenty navzájem porovnány, viz „Tab. 2: Porovnání odpovědí respondentů“. Převažující odpovědi, konkrétní otázky, jsou dále jednotlivě graficky znázorněny.

Tabulka 2: Porovnání odpovědí respondentů[39]

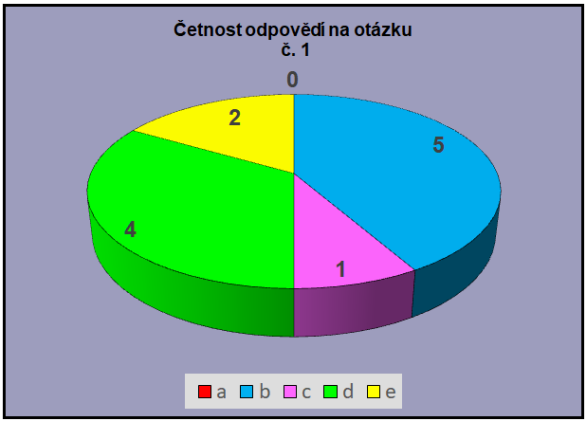
		Odpovědi na otázky									
Resp.	**Oblast působnosti**	**Otázka č. 1**		**Otázka č.2**		**Otázka č. 3**		**Otázka č. 4**		**Otázka č. 5**	
1	Bezpečnostní ředitel zdravotní pojišťovny	b)		a)		a)		b)		a)	
2	Pověřenec pro ochranu osobních údajů	c)		a)		c)		a)		a)	
3	Obchodní ředitel soukr. spol., dodavatele STO	e)		a)		a)		a)		b)	
4	Majitel konsultační spol. v oblasti bezpečnosti	b)		a)		a)		a)		a)	
5	Vedoucí odd. krizového řízení v oblasti dopravy	d)		a)		a)		a)		a)	
6	Bezpečnostní manažer soukr. spol. v oblasti výroby	d)		a)		a)		a)		X*	
7	Bezpečnostní manažer soukr. spol. v oblasti dat. a mob. služeb	b)		a)		c)		a)		a)	
8	Bezpečnostní ředitel společnosti, oblast pohonných hmot	b)		a)		a)		b)		a)	
9	Bezpečnostní ředitel společnosti, oblast telekomunikace	d)		a)		a)		a)		a)	
10	Bezpečnostní ředitel společnosti, oblast hmotných rezerv	b)		a)		a)		a)		a)	
11	Manažer bezpečnosti, oblast životní prostředí	e)		a)		a)		b)		a)	
12	Manažer bezpečnosti, oblast informatiky	d)		a)		c)		a)		b)	
* Respondent nesouhlasí s žádnou odpovědí		a	0	a	12	a	9	a	9	a	9
		b	5	b	0	b	0	b	3	b	2
Vyhodnocení - hodnoty pro jednotlivé grafy		c	1			c	3			c	0
		d	4			d	0			X	1
		e	2								
		Σ	12	Σ	12	Σ	12	Σ	12	Σ	12

„Graf 1: Četnost odpovědí na otázku č. 1“ znázorňuje převahu odpovědí pod písm. b), tj. že, stávající legislativní úpravu v rámci provozování STO v organizacích řízených českým státem, považuje pět respondentů za *dostačující*. Jeden respondent

[39] „Zpracováno autorem.“

uvedl, že stávající legislativa je *nadbytečná*. Čtyři respondenti uvedli, že úprava je *neutěšená* a jeden respondent uvedl, že úprava *neexistuje*.

Graf 1: Četnost odpovědí na otázku č. 1[40]



„Graf 2: Četnost odpovědí na otázku č. 2“ znázorňuje jednoznačnou odpověď pod písm. a), tj. že, respondenti jsou pro, *aby vznikl normativní právní akt*, který by se zabýval ochranou osob a majetku na komerční bázi.

Graf 2: Četnost odpovědí na otázku č. 2[41]

„Graf 3: Četnost odpovědí na otázku č. 3“ znázorňuje převahu odpovědi pod písm. a), tj. že, respondenti jsou pro, aby vznikl normativně právní akt, který by řešil standardizaci základních vnitřních předpisů a dokument má být *samostatným zákonem*.

[40] „Zpracováno autorem.“
[41] „Zpracováno autorem.“

Graf 3: Četnost odpovědí na otázku č. 3[42]

„Graf 4: Četnost odpovědí na otázku č. 4“ znázorňuje převahu odpovědí pod písm. a), tj. že, respondenti jsou pro, *aby vznikl jednotný výklad a uvedení definic bezpečnostní terminologie, a toto bylo součástí normativně právního aktu, viz otázka č. 3*.

Graf 4: Četnost odpovědí na otázku č. 4[43]

„Graf 5: Četnost odpovědí na otázku č. 5“ znázorňuje převahu odpovědí pod písm. a), tj. že, *bezpečnostní manager nebo ředitel by měl být součástí vrcholového managementu* a v normativně právním aktu, byla dána povinnost tuto pozici zřídit.

[42] „Zpracováno autorem.“
[43] „Zpracováno autorem.“

Graf 5: Četnost odpovědí na otázku č. 5[44]

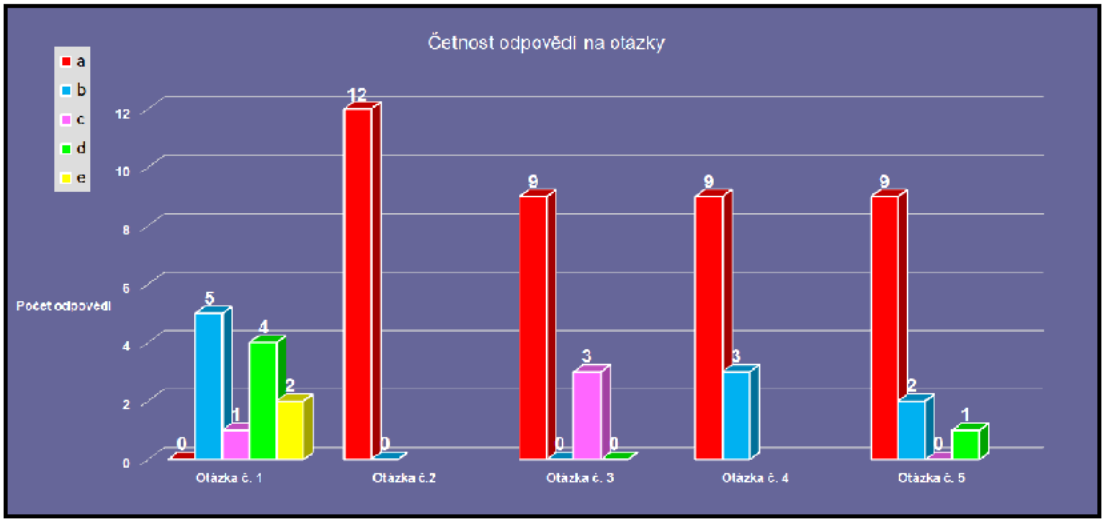
Jeden respondent nesouhlasil s žádnou z odpovědí. K otázce č. 5 uvedl:

„Nesouhlasím s žádnou z odpovědí, protože bychom museli nejdříve definovat, co (kdo) to je vrcholný management a co je to nižší. Je zřejmé, a to lze obecně podpořit, že bezpečnostní manažer (ředitel) by měl být v organizační struktuře zařazen tak, aby mohl odpovědně prosadit bezpečnostní politiku firmy (společnosti). Ideální je, aby byl podřízen přímo řediteli firmy, aby byl v TOP managementu. Podle mne není na závadu, když bezpečnostní manažer bude řešen jako služba a nemusí jít o SBS, ale o bezpečnostní poradenství. Samozřejmě musí být zajištěno, aby externí osoba měla tutéž váhu a vliv jako interní manažer. Podle mne není vyloučena ani varianta, že bezpečnostní manažer nebude v organizační struktuře firmy, ale půjde o externího poradce najatého majitelem firmy a majitel firmy určí jeho postavení a odpovědnost. Jedná se o poměrně složitou otázku, která vydá na samostatnou disertační práci.“

Celkový přehled převažujících odpovědí je graficky znázorněn viz „Graf 6: Výsledný graf výčtových otázek“.

[44] „Zpracováno autorem.“

Graf 6: Výsledný graf výčtových otázek[45]



Výsledek rozhovorů:

U otázky č. 1, sečteme-li kladné a záporné odpovědi, vychází patová situace. **Hlavní hypotéza se nepotvrdila, ani nevyvrátila**.

U otázky č. 2 odpověděli respondenti jednoznačně. **Hlavní a vedlejší hypotéza se potvrdila**. Část respondentů, kteří při první otázce označili, že právní úprava je dostačující nebo nadbytečná, jsou v této otázce proto, aby vznikl samostatný normativní právní akt.

U otázky č. 3 odpověděli respondenti s velkou převahou, kdy jsou pro, aby standardizace základních vnitřních předpisů byla řešena samostatným zákonem. **Hlavní a vedlejší hypotéza se potvrdila**.

U otázky č. 4 odpověděli respondenti s velkou převahou, aby vznikl jednotný výklad a uvedení definic bezpečnostní terminologie a bylo to součástí samostatného zákona. Otázka č. 4 se vázala na otázku č. 3. **Hlavní a vedlejší hypotéza se potvrdila**.

U otázky č. 5 se 11 respondentů z 12 ti vyjádřilo proto, aby bezpečnostní ředitel nebo manažer byl součástí vrcholového managementu. Tato otázka se vázala na otázku č. 4. **Hlavní a vedlejší hypotéza se potvrdila**.

[45] „Zpracováno autorem.“

Analýza k bezpečnostním předpisům:

Autor provedl průzkum u organizací řízených státem v oblasti vnitřních bezpečnostních předpisů, a to formou dotazníku. Dotazník byl vytvořen autorem, pouze pro účely bakalářské práce viz „Tab. 3: Analýza struktury vnitřních bezpečnostních předpisů“. V organizaci, ve které jsem zaměstnán (označuji číslicí 1), jsou zpracované základní bezpečnostní předpisy, dle kterých je zajišťována bezpečnost na více jak na 170 ti objektech v ČR.

Tabulka 3: Analýza struktury vnitřních bezpečnostních předpisů[46]

Průzkum: Analýza struktury vnitřních bezpečnostních předpisů			
V BP nebudou uváděný názvy oslovených společností, budou označeny číslicí 1, 2, 3 ...			
Máte zpracované uvedené předpisy:*		**ANO**	**NE**
1	Bezpečnostní politika		
2	Řízení bezpečnostních rizik		
3	Ochrana informací a osobních údajů		
4	Kybernetická bezpečnost		
5	Řízení bezpečnostních incidentů		
6	Zajištění požární ochrany objektů		
7	Bezpečnostní klasifikace objektů		
8	Provozování a správa STO objektů		
Máte zpracované i jiné bezpečnostní předpisy a jaké:**			
1			
2			
3			
4			
Struktura bezpečnostních předpisů ve vaší společnosti (názvy):***			
1			
2			
3			
4			
5			
6			
7			
8			
9			
*	Názvy předpisů jsou pouze příkladem. Stačí označit, zdali je nebo není uvedená problematika ve vaší společnosti řešena.		
**	Dobrovolné.		
***	Dobrovolné.		

Průzkum se zaměřil na strukturu vnitřních bezpečnostních předpisů u dalších oslovených 6 ti společností (označuji číslicí 2 až 6) s cílem porovnat rozsah těchto předpisů, a zda bezpečnostní problematika uvedená v dotazníku, je společnostmi řešena. V dotazníku je dána možnost dobrovolně uvést i konkrétní vnitřní předpisy, které má společnost vypracovány a také možnost dobrovolně uvést vlastní strukturu bezpečnostních předpisů. Z bezpečnostních důvodů nejsou uváděna jména respondentů a názvy oslovených společností, pouze funkce a oblast působnosti. Ze stejných důvodů nejsou uváděny ani přesné názvy vnitřních bezpečnostních předpisů.

[46] „Zpracováno autorem.“

Respondenti označovali, zdali vyjmenované oblasti bezpečnostní problematiky, jsou nebo nejsou ve společnostech, které v tomto průzkumu zastupují, obsaženy.

Respondent 1 – Bezpečnostní ředitel zdravotní pojišťovny viz „Tab. 4: Respondent 1“ označil všechny kolonky v povinné části. Uvedená problematika je ve společnosti zpracována v samostatných bezpečnostních předpisech. Respondent 1 slouží jako vzorový příklad pro porovnání s dalšími respondenty. Autor je v této společnosti zaměstnán.

Tabulka 4: Respondent 1[47]

Respondent 1			
Máte zpracované uvedené předpisy:*		**ANO**	**NE**
1	Bezpečnostní politika	X	
2	Řízení bezpečnostních rizik	X	
3	Ochrana informací a osobních údajů	X	
4	Kybernetická bezpečnost	X	
5	Řízení bezpečnostních incidentů	X	
6	Zajištění požární ochrany objektů	X	
7	Bezpečnostní klasifikace objektů	X	
8	Provozování a správa STO objektů	X	
*Názvy předpisů jsou pouze příkladem. Stačí označit, zdali je nebo není uvedená problematika ve vaší společnosti řešena.			

Respondent 2 – Pověřenec pro ochranu osobních údajů viz „Tab. 5: Respondent 2“ označil všechny kolonky v povinné části a navíc uvedl názvy čtyř předpisů, které jsou ve společnosti k dané problematice konkrétně zpracovány.

Tabulka 5: Respondent 2[48]

Respondent 2			
Máte zpracované uvedené předpisy:*		**ANO**	**NE**
1	Bezpečnostní politika	X	
2	Řízení bezpečnostních rizik	X	
3	Ochrana informací a osobních údajů	X	
4	Kybernetická bezpečnost	X	
5	Řízení bezpečnostních incidentů	X	
6	Zajištění požární ochrany objektů	X	
7	Bezpečnostní klasifikace objektů	X	
8	Provozování a správa STO objektů	X	
Máte zpracované i jiné bezpečnostní předpisy a jaké:**			
1	Politika bezpečnosti a ochrany zdraví při práci - systém zajištění BOZP		
2	Klasifikace pracovišť a stanovení parametrů pro jejich zabezpečení		
3	Politika informační bezpečnosti		
4	Zajištění požární ochrany		
*Názvy předpisů jsou pouze příkladem. Stačí označit, zdali je nebo není uvedená problematika ve vaší společnosti řešena.			
** Dobrovolné			

[47] „Zpracováno autorem.“
[48] „Zpracováno autorem.“

Respondent 3 – Bezpečnostní ředitel společnosti v oblasti telekomunikací viz „Tab. 6: Respondent 3“ označil všechny kolonky v povinné části a další tři předpisy týkající se krizových situací. V dobrovolné části pak uvedl strukturu bezpečnostních předpisů společnosti.

Tabulka 6: Respondent 3[49]

Respondent 3			
Máte zpracované uvedené předpisy:*		**ANO**	**NE**
1	Bezpečnostní politika	x	
2	Řízení bezpečnostních rizik	x	
3	Ochrana informací a osobních údajů	x	
4	Kybernetická bezpečnost	x	
5	Řízení bezpečnostních incidentů	x	
6	Zajištění požární ochrany objektů	x	
7	Bezpečnostní klasifikace objektů	x	
8	Provozování a správa STO objektů	x	
Máte zpracované i jiné bezpečnostní předpisy a jaké:**			
1	Krizové plány		
2	Krizová dokumentace		
3	Typové plány		
Struktura bezpečnostních předpisů ve vaší společnosti (názvy):***			
1	Strategie		
2	Politiky		
3	Plány		
4	Závazné pokyny		
5	Pracovní zásady		
6	Interní dokumentace		
7	Opatření		
* Názvy předpisů jsou pouze příkladem. Stačí označit, zdali je nebo není uvedená problematika ve vaší společnosti řešena.			
** Dobrovolné.			
*** Dobrovolné.			

Respondent 4 – Vedoucí oddělení krizového řízení v oblasti dopravy viz „Tab. 7: Respondent 4“ označil v povinné části, v jedné kolonce, že problematiku provozování STO neřeší v samostatném předpise, ale ve dvou, které vyjmenoval.

Tabulka 7: Respondent 4[50]

Respondent 4			
Máte zpracované uvedené předpisy:*		**ANO**	**NE**
1	Bezpečnostní politika	X	
2	Řízení bezpečnostních rizik	X	
3	Ochrana informací a osobních údajů	X	
4	Kybernetická bezpečnost	X	
5	Řízení bezpečnostních incidentů	X	
6	Zajištění požární ochrany objektů	X	
7	Bezpečnostní klasifikace objektů	X	
8	Provozování a správa STO objektů		X
Máte zpracované i jiné bezpečnostní předpisy a jaké:**			
1	Směrnice na ochranu osob a majetku		
2	Směnice pro používání kamerových systémů		
* Názvy předpisů jsou pouze příkladem. Stačí označit, zdali je nebo není uvedená problematika ve vaší společnosti řešena.			
** Dobrovolné.			

[49] „Zpracováno autorem.“
[50] „Zpracováno autorem.“

Respondent 5 – Bezpečnostní ředitel v oblasti hmotných rezerv viz „Tab. 8: Respondent 5“ označil všechny kolonky v povinné části a uvedl další tři předpisy, které mají ve společnosti zpracované. V dobrovolné části pak uvedl, že strukturu bezpečnostních předpisů ve společnosti řeší formou procesů dle ISO 9001.

Tabulka 8: Respondent 5[51]

Respondent 5			
Máte zpracované uvedené předpisy:*		**ANO**	**NE**
1	Bezpečnostní politika	x	
2	Řízení bezpečnostních rizik	x	
3	Ochrana informací a osobních údajů	x	
4	Kybernetická bezpečnost	x	
5	Řízení bezpečnostních incidentů	x	
6	Zajištění požární ochrany objektů	x	
7	Bezpečnostní klasifikace objektů	x	
8	Provozování a správa STO objektů	x	
Máte zpracované i jiné bezpečnostní předpisy a jaké:**			
1	Personální bezpečnost		
2	IT bezpečnost - vše co je mimo zákon a vyhlášku o KB		
3	ochrana utajovaných informací		
Struktura bezpečnostních předpisů ve vaší společnosti (názvy):***			
1	**dle ISO 9001 - formou procesů**		
* Názvy předpisů jsou pouze příkladem. Stačí označit, zdali je nebo není uvedená problematika ve vaší společnosti řešena.			
** Dobrovolné.			
*** Dobrovolné.			

Respondent 6 – Manažer bezpečnosti v oblasti informatiky viz „Tab. 9: Respondent 6“ označil všechny kolonky v povinné části a uvedl další tři předpisy, které mají ve společnosti zpracované.

Tabulka 8: Respondent 6[52]

Respondent 6			
Máte zpracované uvedené předpisy:*		**ANO**	**NE**
1	Bezpečnostní politika	✓	
2	Řízení bezpečnostních rizik	✓	
3	Ochrana informací a osobních údajů	✓	
4	Kybernetická bezpečnost	✓	
5	Řízení bezpečnostních incidentů	✓	
6	Zajištění požární ochrany objektů	✓	
7	Bezpečnostní klasifikace objektů	✓	
8	Provozování a správa STO objektů	✓	
Máte zpracované i jiné bezpečnostní předpisy a jaké:**			
1	Uplatnění práv Subjektů osobních údajů (směrnice)		
2	Zabezpečení ochrany osob a majetku (směrnice)		
3	Zajištění ochrany dat a zabezpečení režimového pracoviště (směrnice)		
* Názvy předpisů jsou pouze příkladem. Stačí označit, zdali je nebo není uvedená problematika ve vaší společnosti řešena.			
** Dobrovolné.			

[51] „Zpracováno autorem.“
[52] „Zpracováno autorem.“

Výsledek analýzy bezpečnostních předpisů:

Autor se touto analýzou, která byla provedena v omezeném rozsahu, nepokoušel o hlubší zkoumání, které by mělo mít vliv na stanovené cíle. Provedená analýza měla za cíl ověřit, zda i přes neexistenci právní normy, jsou bezpečnostní problematiky ve společnostech řízené státem, vnitřními předpisy obsaženy. Výsledek zkoumání lze subjektivně ohodnotit velmi pozitivně.

9 Shrnutí praktické části

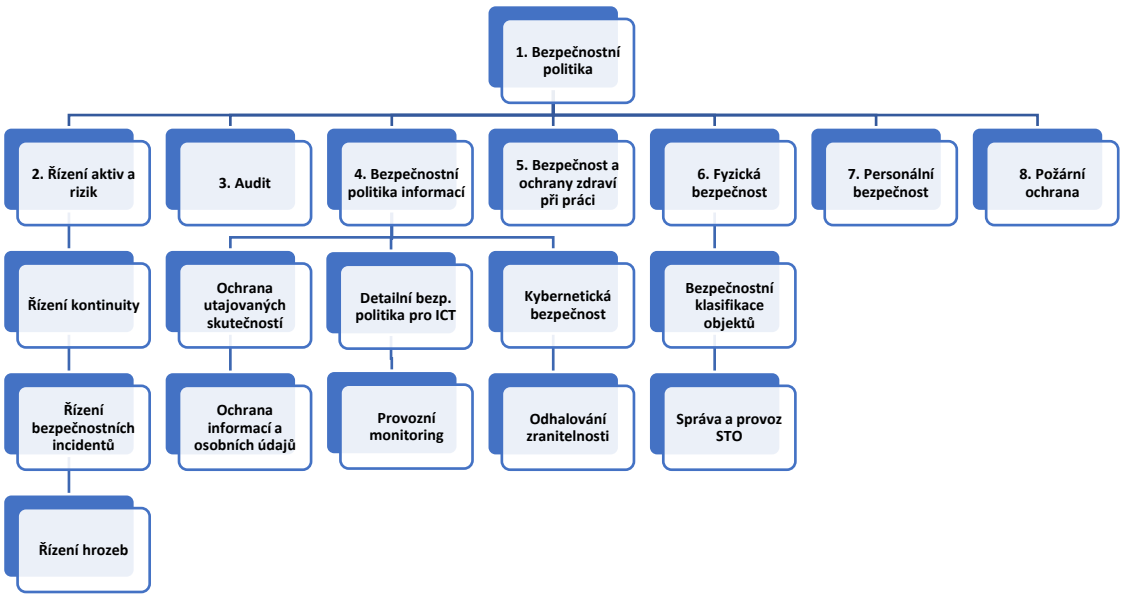
Výsledkem rozhovorů se nepotvrzuje ani nevyvrací hlavní hypotéza, tedy, že v ČR není dostatečně upravena legislativa pro provoz STO. Tímto se, mimo výzkum autora, potvrzuje veřejně známý nesoulad bezpečnostní komunity ČR v oblasti legislativy. V dalších otázkách pak respondenti naopak s velkou převahou potvrzují nutnost vydat samostatný zákon o SBS, standardizovat bezpečnostní terminologii, ale i základní strukturu bezpečnostních předpisů, a to taktéž samostatným zákonem. Hlavní i vedlejší hypotéza se potvrdila.

Šesti respondentům (zaměstnanci státních organizací), se kterými byli vedeny rozhovory, byl předložen i dotazník k analýze vnitřních bezpečnostních předpisů organizací ve kterých působí. Výsledek potvrzuje, že bezpečnostní ředitelé a manažeři organizací řízených státem mají zpracované vnitřní bezpečnostní předpisy, které plně pokrývají po obsahové stránce problematiku vnitřní bezpečnosti.

10 Návrh struktury dokumentů v oblasti zajištění vnitřní bezpečnosti

Organizační struktura bezpečnostních politik organizace je budována s pomocí interních specialistů, kteří jsou zodpovědní za tuto oblast. Vnitřní bezpečností předpisy, nebo-li bezpečnostní politiky je termín, který je bezpečnostní komunitou vnímán a prezentován jako standard a nezbytný souhrn organizačních pravidel pro zajištění a zvýšení bezpečnosti v organizaci. Autor navrhuje, jako vedlejší cíl bakalářské práce viz „Obr. 8: Základní struktura bezpečnostních předpisů“, přehled základních oblastí, na které by měla mít každá organizace vypracované konkrétní směrnice, předpisy nebo postupy.

Obrázek 8: Základní struktura bezpečnostních předpisů[53]



1. Bezpečnostní politika a její význam viz. čl. 5 str. 36.
2. Řízení aktiv a rizik jsou procesy, které spojují řadu různorodých oblastí a agent, jsou nedílnou součástí rozvoje bezpečnosti organizace.
3. Audit je standardizované prověření bezpečnostní dokumentace a příslušných opatření.
4. Bezpečnostní politika informací je soubor dokumentů, které určují, jak chce organizace čelit rizikům. Stanovuje cíle a způsoby zabezpečení informací.
5. BOZP je souhrn opatření, jimiž zaměstnavatel eliminuje vznik rizik na pracovišti, jak pro zaměstnance, tak i pro ostatní fyzické osoby.
6. Fyzická bezpečnost tvoří systém organizačních a technických opatření, které jsou zaměřeny na ochranu aktiv organizace.
7. Personální bezpečnost je základním druhem zajištění ochrany informací. Stav, kdy zaměstnanci jednaní tak, aby neohrozili citlivé informace.
8. Požární ochrana je aplikací technických, ale i netechnických prostředků prevence vzniku požáru.

[53] „Zpracováno autorem.“

Závěr

Teoretická část bakalářské práce se zaměřila na představení systémů technické ochrany a snažila se přiblížit základy objektové bezpečnosti a z jakých důvodů se technická ochrana objektu realizuje. Ve státních organizacích před samotnou instalací bezpečnostních systémů, musí dojít k procesu, který specifikuje postupy, jak jednotlivá aktiva chránit. K tomuto účelu slouží bezpečnostní politiky společnosti a k nim zpracovaná pravidla ve formě vnitřních předpisů. Jedná se zejména o analýzu rizik a hrozeb, na jejímž základě lze určit způsob a rozsah zabezpečení. Důležitou roly v prosazování bezpečnostních politik hraje postavení bezpečnostního manažera v hierarchii společnosti, která byla zejména v minulosti silně podceňována. V dnešní době je situace bezpečnostních manažerů o něco příznivější, a to díky celkovému vývoji v oblasti např. kybernetické bezpečnosti, ochraně osobních údajů a v neposlední řadě v samotném vývoji bezpečnostních systémů.

Praktická část se zabývá problematikou neexistence jednotné legislativní úpravy o technické ochraně objektů, kterou v současné době zajišťují soukromé bezpečnostní služby. České soukromé bezpečnostní služby nemají dosud, jako jediné v EU vlastní legislativní úpravu. Slovenská republika má již vydaný zákon o soukromých bezpečnostních službách, po kterém mi v České republice několik let marně voláme. Zajištění bezpečnosti objektů představuje víceoborovou činnost, v níž podcenění jakékoliv části může vést k významným ztrátám na aktivech společnosti. Aktuálně vydané zákony, zabývající se komerční objektovou bezpečností, neobsahují povinnost mít zpracované vnitřní bezpečnostní politiky, nejsou standardizované a nejsou ani povinné. Není-li povinnost, nemusí být kontrola a sankce je tak nevymahatelná. Náprava se pak řeší až ex post. Při řešení bezpečnosti státních organizací nebo společností, by se mělo uplatňovat komplexní pojetí. Soukromé bezpečnostní společnosti musí mít pro praxi jasná a definovaná pravidla. Profesní bezpečnostní komunita stále trpí terminologickou a legislativní nejednotností. Vznikem standardizovaného právního aktu dojde k podstatnému zlepšení řízení bezpečnostního prostředí, a to nejen v organizacích řízených českým státem. Může dojít i k lepšímu postavení a pochopení bezpečnostních ředitelů nebo manažerů v očích vrcholového managementu.

Na samotný závěr bych chtěl poznamenat, že tato bakalářská práce může být přínosem a pomůckou pro začínající pracovníky v oblasti komerční bezpečnosti nebo bezpečnostního managementu.

Seznam použitých zdrojů

Literární zdroje

1. BALABÁN, M., STEJSKAL, L. *Kapitoly o bezpečnosti.* Praha: Karolinum, 2019. 484 s. ISNB 978-80-246-1863-0.
2. BALABÁN, M., PERNICA, B. *Bezpečnostní systémy ČR: problémy a výzvy.* Praha: Karolinum, 2015. 312 s. ISBN 978-80-246-3150-9.
3. DANICS, Š. *Bezpečnostní politika ve veřejné správě.* České Budějovice: VŠERS, 2007. 99 s. ISBN 978-80-86708-38-6.
4. FRYŠAR, M. a kolektiv. *Bezpečnost pro manažery, podnikatele a politiky*. Praha: Public History Praha, 2006. 176 s. ISBN 80-86445-22-4.
5. IVANKA, J., *Mechanické zábranné systémy*. 2. vydání. Zlín: Univerzita Tomáše Bati ve Zlíně, 2014. 148 s. ISBN 978-80-7454-427-9.
6. KAMENÍK, J., BRABEC, F., a kolektiv. *Komerční bezpečnost.* 2. vydání. Praha: Wolters Kluwer ČR, 2019. 344 s. ISBN 978-80-7598-303-9.
7. KOLOUCH, J., BAŠTA, P. a kolektiv. *CyberSecurity*. 1. vydání. Praha: CZ.NIC, 2019. 560 s. ISBN 978-80-88168-34-8.
8. KRULIŠ, J., *Jak vítězit nad riziky. Aktivní management rizik – nástroj řízení úspěšných firem.* Praha: Linde Praha a.s., 2011. 568 s. ISBN 978-80-7201-835-2.
9. KYNCL, J., a kolektiv. *Bezpečnost objektu ve světle moderních technologií.* Praha: KPKB ČR, 2014. 400 s. ISBN 978-80-260-7115-0.
10. LOVEČEK, T., REITŠPÍS, J. *Projektovanie a hodnotenie systémov ochrany objektov*. SK. Žilina: EDIS, 2011. 281 s. ISBN 978-80-554-0457-8.
11. LUKÁŠ, L., a kolektiv. *Bezpečnostní technologie, systémy a management II.* 1. vydání. Zlín: VeRBuM, 2012. 387 s. ISBN 978-80-87500-19-4.
12. LUKÁŠ, L., a kolektiv. *Bezpečnostní technologie, systémy a management III.* 1. vydání. Zlín: VeRBuM, 2013. 456 s. ISBN 978-80-87500-35-4.
13. LUKÁŠ, L., a kolektiv. *Bezpečnostní technologie, systémy a management IV.* 1. vydání. Zlín: VeRBuM, 2014. 390 s. ISBN 978-80-87500- 57-6.
14. PORADA, V., a kolektiv. *Bezpečnostní vědy*. Plzeň: Aleš Čeněk, 2019. 780 s. ISBN 978-80-7380-758-0. VILÁŠEK, J., FUS, J. Krizové řízení v ČR na počátku 21. století. Praha: Karolinum, 2012. 264 s. ISBN 978-80-264-2170-8.

15. VILÁŠEK, J., FUS, J. *Krizové řízení v ČR na počátku 21. století*. Praha: Karolinum, 2012. 264 s. ISBN 978-80-264-2170-8.

Elektronické zdroje

1. *Česká bezpečnostní terminologie, Výklad základních pojmů.* ÚSTAV STRATEGICKÝCH STUDIÍ VOJENSKÉ AKADEMIE V BRNĚ, 2002. https://moodle.unob.cz/pluginfile.php/11277/course/section/3043/%C4%8Cesk%C3%A1%20bezpe%C4%8Dnostn%C3%AD%20terminologie.pdf.
2. ÚOOÚ – *K provozování kamerových systémů.* https://www.uoou.cz/k-provozovani-kamerovych-systemu/d-29535.
3. HALOUZKA, K. *Fyzická bezpečnost. Téma Perimetrické zabezpečovací systémy.* https://docplayer.cz/4405209-Fyzicka-bezpecnost-tema-perimetricke-zabezpecovaci-systemy-ing-kamil-halouzka-ph-d-kamil-halouzka-unob-cz.html.
4. HOLEČEK, M. předseda ÚNMZ, Moderní evropský standart zabezpečení. *Sborník technické harmonizace 2013*. http://www.azks.cz/data/clanky/files/000140.pdf.
5. KOKTAN, P. *Nové označení bezpečnostních tříd mechanických zábranných systémů není jen prekabatenie.* https://www.bezpecnostni-dvere-mrize-kavan.cz/wp-content/uploads/2013/03/secmag_1-2013aga-WEB-kopie.png.
6. *Technologické trendy roku 2020,* podle společnosti Cisco Systém. https://ictrevue.hn.cz/c3-66706960-0ICT00_d-66706960-technologicke-trendy-roku-2020-podle-spolecnosti-cisco-systems.
7. PORADA, V., BRUNA, E. *Bezpečná Evropa 2018.* 1. vydání. Praha: VŠFS, 2018. 546 s. ISBN 978-80-7408-185-9. https://www.vsfs.cz/prilohy/konference/sbornik_be2018.pdf.

Legislativní dokumenty

1. Zákon č. 473/2005 Z. z. Zákon o poskytovaní služieb v oblasti súkromnej bezpečnosti a o zmene a doplnení niektorých zákonov (zákon o súkromnej bezpečnosti) https://www.zakonypreludi.sk/zz/2005-473.

Ostatní zdroje

1. Nařízení Evropského parlamentu a Rady (EU) ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

Seznam zkratek

CCTV	Closed Circuit Television (uzavřený televizní okruh)
BOZP	Bezpečnost a ochrana zdraví při práci
BPO	Bezpečnostní posouzení objektu
DPPC	Dohledové poplachové a přijímací centrum (SBS a PČR)
EKV	Elektronická kontrola vstupu
EPS	Elektrické požární systémy
EU	Evropská unie
GB/s	Giga Bit za sekundu je jednotka přenosové rychlosti
GPRS	General Packet Radio Service (umožňuje mobilním telefonům přenos dat a připojení k internetu)
GSM	Group Spécial Mobile (buňková mobilní síť)
HZS	Hasičský záchranný sbor
ICT	Information and Communication Technologies (informační a komunikační technologie)
ID	Identity Document (identifikační karta pro přístupové elektronické systémy)
IP	Internet Protocol (základní protokol používaný v počítačových sítích a internetu)
ISDN	Integrated Services Digital Network (digitální síť internetových služeb)
IZS	Integrovaný záchranný systém (HZS, ZSS a PČR)
MZS	Mechanické zábranné systémy
PA	Požární alarm

PBŘ	Požárně bezpečnostní řešení stavby
PCO HZS	Pult centrální ochrany provozovaný HZS
PO	Požární ochrana
PTV	Průmyslová televize
PZTS	Poplachové zabezpečovací a tísňové systémy
RC	Resistence classes (bezpečnostní třída)
SBS	Soukromá bezpečnostní služba
STO	Systémy technické ochrany
ÚNMZ	Úřad pro technickou normalizaci, metrologii a státní zkušebnictví
ÚOOÚ	Úřad pro ochranu osobních údajů
VSS	Video Surveillance Systém (dohledové videosystémy)
ZZS	Zdravotnická záchranná služba

Seznam obrázků

Seznam tabulek

Seznam grafů

Seznam příloh

1) Považujete stávající legislativní úpravu v rámci provozování STO v organizacích řízených českým státem za:

   a) srozumitelnou,

   b) dostačující,

   c) nadbytečnou,

   d) neutěšenou,

   e) úprava neexistuje.

2) V současnosti neexistuje v ČR (oproti SR) normativní právní akt, který by se zabýval ochranou osob a majetku na komerční bázi:

   a) byl byste proto, aby takový to normativní právní akt v ČR vznikl,

   b) nebo si myslíte, že je nadbytečný.

3) Pokud jste pro, aby normativně právní akt, který by řešil standardizaci základních vnitřních předpisů vznikl, dokument má být:

   a) samostatným zákonem,

   b) sloučen ve společném zákoně,

   c) vyhláškou MV ČR,

   d) jiným dokumentem.

4) V současné době je i nejednotná terminologie bezpečnostního názvosloví např. co přesně znamená bezpečnostní událost, incident, opatření apod., MZP - mechanické zábranné prostředky a MZS - mechanické zábranné systémy aj.:

   a) byl byste proto, aby vznikl jednotný výklad a uvedení definic bezpečnostní terminologie, a toto bylo součástí normativně právního aktu, viz otázka č. 3,

   b) nebo postačí terminologie uvedené ve vydaných ČSN-EN týkající se STO.

5) Byl by jste proto, aby v normativně právním aktu, byla dána povinnost zřídit bezpečnostního manažera/ředitele a tuto funkci zařadit na úroveň vrcholového managementu:

   a) bezpečnostní manager nebo ředitel by měl být součástí vrcholového managementu,

   b) postačí pozice nižšího managementu a nemusí být součástí vrcholového managementu,

   c) bezpečnostní manager by měl být řešen dodavatelsky za využití SBS.