Zabezpečovací systémy ve vztahu k utajovaným informacím

Tomáš Wencel

Bakalářská práce
2023

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva

Akademický rok: 2022/2023

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Tomáš Wencel**
Osobní číslo:	**L20269**
Studijní program:	**B1032A020002 Ochrana obyvatelstva**
Forma studia:	**Kombinovaná**
Téma práce:	**Zabezpečovací systémy ve vztahu k utajovaným informacím**

Zásady pro vypracování

1. Zpracujte teoretický vstup do dané problematiky.
2. Analyzujte současný stav zabezpečení ve vybraném objektu/místnosti.
3. Navrhněte možné zlepšení bezpečnosti s ohledem na utajované informace.

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

Seznam doporučené literatury:

1. BURDA, Karel. *Základy elektronických zabezpečovacích systémů*. Brno: Akademické nakladatelství CERM, 2017. ISBN 978-807-2049-677.
2. ČSN EN 50131-2-10 (334591). *Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 10: Aplikace specifických požadavků na komunikátor ve střeženém prostoru (SPT)*. Praha: Českou agenturu pro standardizaci, 2019.
3. MATIC, Luka. *Electronic Security and Espionage*. London: Elektor Verlag. 2021. ISBN 3895764655.
4. HONEY, Gerard. *Electronic Security Systems Pocket Book*. Newnes, 1999. ISBN 13: 9780750639910.

Další odborná literatura dle doporučení vedoucí bakalářská práce.

Vedoucí bakalářské práce: **Ing. Martin Ficek**
Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: **1. prosince 2022**
Termín odevzdání bakalářské práce: **5. května 2023**

L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2022

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

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

V Uherském Hradišti, dne: 5.5.23

Jméno a příjmení studenta: Tomáš Wencel

.....
podpis studenta

ABSTRAKT

Tématem této bakalářské práce jsou zabezpečovací systémy ve vztahu k utajovaným informacím. Teoretická část definuje základní pojmy utajovaných informací, rozdělení bezpečnosti a úzce definuje zabezpečovací systémy. Teoretická část je zakončena analýzou rizik, kde jsou popsány metody brainstormingu a analýzy možných vad a následků.

Praktická část se věnuje vybranému objektu X, který je podrobně popsán a pomocí analýzy FMEA (analýza možných vad a následků) zanalyzován z pohledu návrhu zabezpečení objektu tak, aby mohl objekt pracovat v režimu utajení se stupněm Vyhrazené a Důvěrné. Závěr praktické části je věnován shrnutí provedené analýzy.

Klíčová slova: utajovaná informace, zabezpečovací systémy, bezpečnost, bezpečnost (personální, administrativní, fyzická), analýza rizik

ABSTRACT

The topic this bachelor thesis is security systems in relation to classified information. The theoretical part defines the basic concepts of classified information, the division of security and narrowly defines security systems. The theoretical part ends with a risk analysis, where Brainstorming and Failure Mode and Effects Analyses.

The practical part is devoted to the selected object X, which is described in detail and analysed by means od FMEA (Failure Mode and Effects Analyses) from the point of view of designing the security of the object so that it can operate in the classified mode with the classification level of Restricted and Confidential. The conclusion of the practical part is devoted to a summary of the analysis.

Keywords: classified information, security systems, security, security (personnel, administrative, psysical), risk analysis

Chtěl bych poděkovat za veškerou trpělivost a ochotu svému vedoucímu bakalářské práce Ing. Martinu Fickovi Ph.D., za jeho cenné rady, vřelou komunikaci a čas, který si pro mě vyhradil.

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

OBSAH

ÚVOD

Zabezpečovací systémy a utajované informace jsou dva silné pojmy, bez kterých se řada lidí neobejde. Ať už jde o to, jakým způsobem utajovanou informaci chránit, nebo jak práce s utajovanými informacemi dokáže ovlivňovat zabezpečovací systémy. Správná volba jakéhokoliv zabezpečovacího systému může ovlivnit složitost krádeže nebo zneužití utajované informace, což může mít za následek újmu nevyčíslitelné hodnoty. Každodenní práce s informacemi dala impuls k rozboru témat jak, kdy, kde a hlavně kdo může pracovat s určitými informacemi a jak tyto informace zabezpečit. Jako odpovědi na tyto otázky vznikly termíny zabezpečovací systémy a utajovaná informace. Vznikly seznamy informací, které nejsou nebo nemohou být veřejnosti přístupné a byl vytvořen návod, jak je chránit.

Bakalářská práce má za cíl přiblížit problematiku zabezpečovacích systémů přenesených na určitý objekt, ve kterém se má chránit utajovaná informace. Vše pomocí analýzy možných vad a následků.

Teoretická část pojednává o zabezpečovacích systémech a jejich rozdělení a použití v praxi. Přičemž do těchto systémů patří poplachové zabezpečovací a tísňové systémy, které mají za úkol zabezpečit vybraný objekt pomocí elektronických čidel, detektorů a kontaktů, dále elektronická kontrola vstupů, která hlídá a vede záznamy o vstupujících do vybraných místností či objektů, elektronická požární signalizace, která má za úkol hlídat a detekovat stav budovy při vzniku požáru, kamerový systém, jenž lze využít jako vizuální dohled nad střeženým objektem a mechanické zábranné systémy, které slouží k přispění odolnosti objektu a zabránění vstupu možných pachatelů. Všechny tyto systémy lze aplikovat na zabezpečení utajovaných informací a jejich bezpečnosti, což je pokračování praktické části této bakalářské práce. Za utajovanou informaci můžeme považovat cokoliv, co vybraný objekt, který s takovou informací smí nakládat, označí jako utajovanou informaci s ohledem na to, že taková informace a její manipulace, uchovaní a likvidace podléhá konkrétní bezpečnosti.

Praktická část se věnuje popisu objektu X, který přechází do režimu práce s utajovanými informacemi, proto je pro tento objekt důležité zanalyzovat, jak a jakými prostředky tomuto objektu zvýšit bezpečnostní odolnost – a to za pomocí brainstormingu, kterého se účastní certifikované firmy a odborník na analýzu možných vad a následků. Společně s ředitelem instituce se vyplní protokoly analýzy FMEA a určí se rizikové číslo každé vady. Závěr praktické části se věnuje shrnutí analýzy a návrhu zlepšení zabezpečovacích systémů na konkrétní objekt X.

I. TEORETICKÁ ČÁST

1 ZABEZPEČOVACÍ SYSTÉMY

„V dnešní době jsou bezpečnostní systémy jen zřídkakdy řádně řešeny nebo správně vyřešeny. Například elektronické zabezpečení je pouze součástí řetězce, který zajišťuje bezpečnost systému, opomíjejí se však ostatní aspekty, ale řetěz je tak silný, jak jeho nejslabší článek.“ (Matic, 2021)

Kapitola pojednává o celkovém rozdělení zabezpečovacích systému. Do těchto systému patří:

1) poplachové zabezpečovací a tísňové systémy,
2) elektronická kontrola vstupů,
3) elektronická požární signalizace,
4) kamerové systémy,
5) mechanické zábranné systémy.

1.1 Poplachový zabezpečovací a tísňový systém

Poplachový zabezpečovací a tísňový systém (dále jen PZTS) spadá pod normu ČSN EN 50131-2-10 (334591) a normu TNI 33 4591, která je právně nezávazná, slouží jako návod k instalaci a zacházení se systémem. Jde o elektronické bezpečnostní systémy, které pracují v oblasti života, zdraví a majetku osob, společností a státních institucích. Základním cílem je detekce a včasné upozornění na potenciální nebo probíhající nežádoucí událost ve střežené oblasti. Za nežádoucí událost můžeme považovat narušení kontrolované oblasti osobami bez povolení vstupu, únik z kontrolované oblasti, neoprávněná manipulace s předmětem, který je chráněn, nebo také detekce požáru, úniky vody a úniky nebezpečných látek (ČSN EN 50131-2-10 (334591), 2019, Burda, 2017).

Norma uvádí čtyři stupně zabezpečení dle stupně rizika:

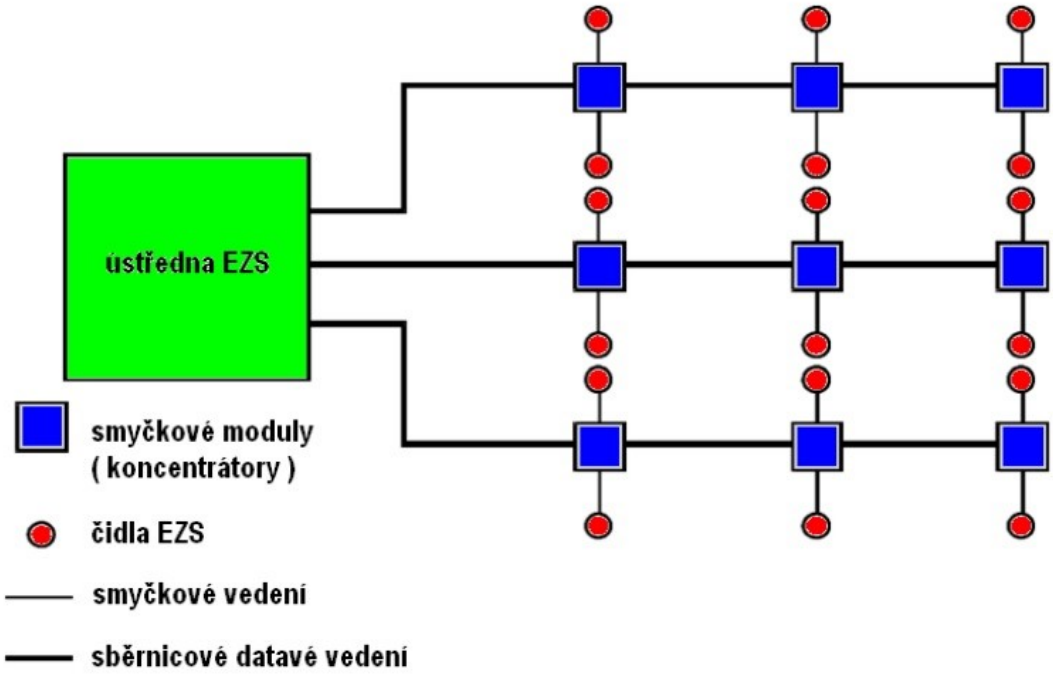
1) nízké riziko – rodinné doma, byty, garáže,
2) nízké až střední – komerční objekty,
3) střední až vysoké – památky, zbraně, peněžní ústavy, směnárny,
4) vysoké riziko – objekty vyššího významu (státní instituce, jaderné zařízení).

Tyto bezpečnostní třídy definují charakter prostoru, kde je systém instalován a kladou podle nich požadavky pomocí norem, kdy jde o zálohování systému, technické parametry použitých komponentů a oblasti, které mají být chráněny (Pokorný, 2019).

Struktura PZTS se staví na propojení ústředny s ostatními prvky systému, od kterých ústředna získává a podle nastavených parametrů vyhodnocuje příchozí signály. Poplachový zabezpečovací a tísňový systém je jen nástroj k detekci vzniklého problému na chráněném objektu, nikoli jeho řešení. V případě, že v objektu není nepřetržitá obsluha, využívá se k ostraze bezpečnostní agentura, která vše sleduje na dálku a po vyhlášení poplachu zakročí. Tyto agentury využívají propojení PZTS s dohledovým poplachovým a přijímacím centrem (dále jen DPPC). Dohledové poplachové a přijímací centrum a PZTS jsou propojeny pomocí GSM modulů, objekt je tak sledován nepřetržitě obsluhou DPPC a ta v případě poplachu volá bezpečnostní agenturu, nebo policii (Lukáš, 2015).

Rozdělení ústředen

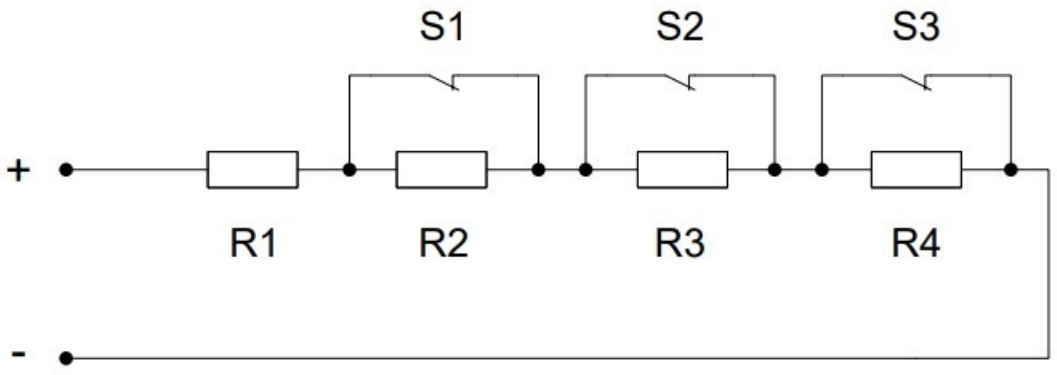
Ústředny PZTS se rozdělují do čtyř kategorií: ústředny smyčkového typu, ústředny s přímou adresací a ústředny smíšeného typu. Poslední zmíněná ústředna je kombinací dvou předchozích ústředen, a proto je v dnešní době nejvyužívanější ústřednou pro instalaci PZTS. Její koncové prvky systému (čidla a magnety) tvoří samostatně uzavřené proudové smyčky, které jsou spojeny v tak zvaných expandérech a ty následně pomocí sběrnice komunikují s hlavní ústřednou. Nejčastěji se setkáváme s typem sběrnice RS-485. Posledním typem jsou ústředny s bezdrátovým přenosem poplachového signálu od čidel (Lukáš, 2015).



Obrázek 1 – zapojení systému EZS s ústřednou smíšeného typu (Hladík, 2011)

Koncové prvky poplachových zabezpečovacích a tísňových systémů

Provedení a zaměření koncových prvků se liší, ale způsob, jakým stylem vyhlašují poplach, je společný. Jde o jednoduchý elektrický obvod (Křeček, 2003).



Obrázek 2 – schématické zapojení prvků PZTS (Křeček, 2003)

Samostatné snímače se rozdělují do různých kategorií. Jsou využívány při volení správného čidla pro oblast, která se má chránit. Dělení prvků:

1) plášťové ochrany – čidla na ochranu skleněných ploch, magnetické kontakty, mechanické kontakty, vibrační čidla, poplachové folie, tapety, drátová čidla a rozpěrné tyče,
2) prostorové ochrany – pasivní infračervená čidla, aktivní infračervená čidla, ultrazvuková čidla, mikrovlnná čidla, kombinovaná duální čidla,
3) tísňové ochrany – tísňové hlásiče veřejné, skryté, osobní,
4) perimetrické (obvodové) ochrany – zemní tlakové hadice, perimetrická pasivní infračervená čidla, štěrbinové kabely, mikrovlnné bariéry, infračervené závory a bariéry, mikrofonické kabely,
5) předmětové ochrany – polohová čidla, kapacitní čidla, otřesová čidla, čidla na ochranu závěsných předmětů,
6) prvky speciální ochrany – nášlapné koberce, tlaková čidla, polohová čidla (Vávra, 2020).

Ovládací zařízení

Tyto prvky jsou důležité pro PZTS a jeho funkci. Uvádějí celý systém do stavu zabezpečení a klidového stavu. Patří k nim zejména:

1) kódové klávesnice,
2) spínací a blokovací zámky,
3) ovládací a indikační zámky (Vávra, 2020).

1.2 Elektronická kontrola vstupů

„Elektronická kontrola vstupu má své uplatnění všude tam, kde je nutné kontrolovat a regulovat přístup osob do objektu nebo jeho částí. Autorizovaným osobám umožní po identifikaci přístup do příslušných prostor, zatímco ostatním není přístup do těchto částí povolen.“ (Trade fides, 2019)

Elektronická kontrola vstupů (dále jen EKV) a její technické parametry prvků jsou uvedeny v ČSN EN 60839-11-1 (334593). Systémy EKV spolu s PZTS jsou děleny dle chráněného prostoru do bezpečnostní třídy dle normy ČSN EN 50131–1 ED.2 (334591), systémy EKV jsou i předmětem zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, poněvadž všechny prostory uvedené v tomto zákoně vyžadují instalaci EKV (Kolouch, Bašta, 2019).

Prvky elektronické kontroly vstupů

Systém EKV má za účel identifikovat a kontrolovat osoby s přístupem do chráněného objektu. V součinnosti tří zařízení vzniká funkční systém pro vstup nebo odepření vstupu. Mezi tyto zařízení patří:

1) pro identifikaci osob – čtečky karet, otisky prstů aj.,
2) zábranné prostředky – elektronické zámky, pohony bran aj.
3) zařízení pro vyhodnocování signálů – ústředny, dveřní jednotky (Kolouch, Bašta, 2019).

1.3 Elektronická požární signalizace

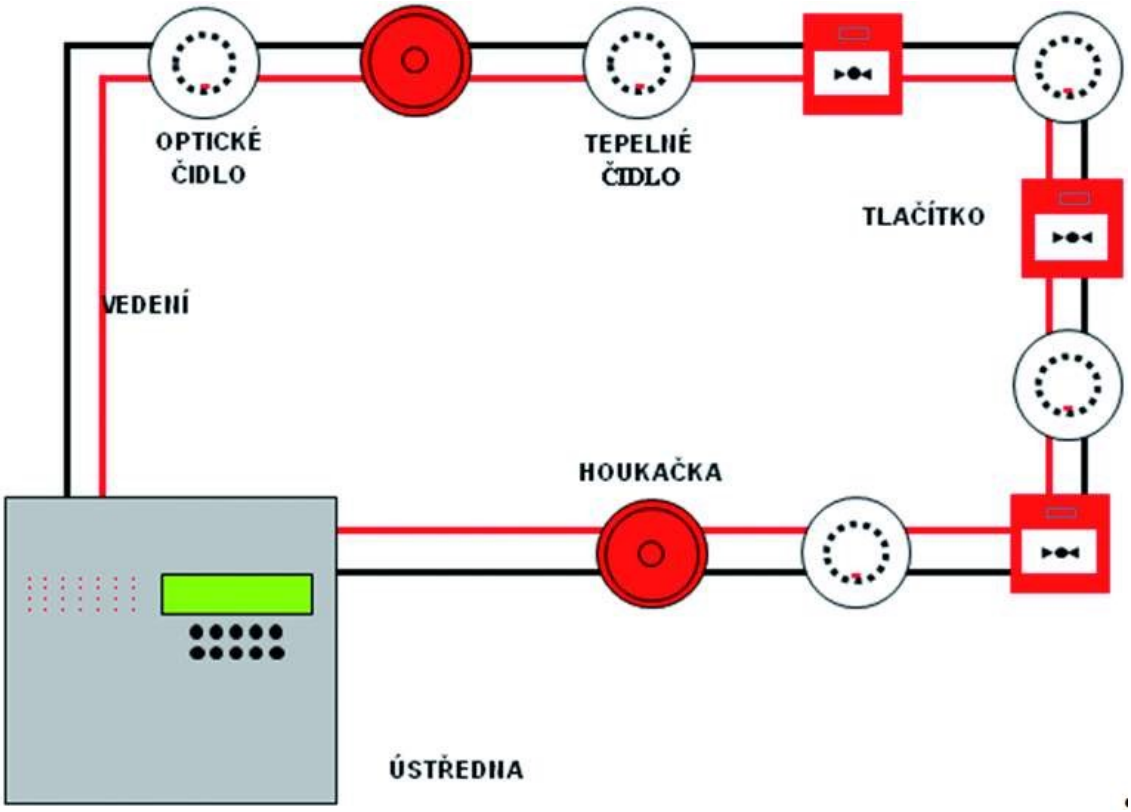
K detekci požáru nám slouží soubor technických zařízení nazývaný elektronická požární signalizace (dále jen EPS). Jejím účelem je včasné detekování požáru již při jeho vzniku, přivolání odpovědné osoby, která může oheň zlikvidovat nebo přivolat pomoc. Mezi hlavní úkoly EPS patří rychlé a spolehlivé určení místa, kde je detekováno počáteční zahoření. Dalším úkolem EPS je vyhlašování poplachu při detekci, řízení evakuačního systému v místech či oblastech, která jsou zasažena a neméně významnou součástí EPS je automatický systém komunikace s hasičským záchranným sborem (dále jen HZS). Tento systém komunikace je zařazen do integrovaných bezpečnostních a havarijních systémů ochrany majetku a osob (Hladík, 2011).

Elektronická požární signalizace patří mezi základní součásti systému požárně bezpečnostního zařízení, poněvadž význam EPS v mnoha případech předčí ostatní zabezpečovací systémy, ať už jde o ochranu majetku nebo ochranu života a zdraví osob. Elektronická požární signalizace je tvořena taktéž ústřednou, která funguje jako mozek celého systému a na ni jsou navázány různé typy hlásičů, koncová a ovládací zařízení, která informují obsluhu o vznikajícím požáru akustickooptickou signalizací přímo v objektu nebo za pomoci dálkového přenosu na pult centrální ochrany (dále jen PCO), který je umístěn u HZS (Hladík 2011).

Systémy EPS se instalují buď jako samostatné aplikace nebo jako součást vyššího integrovaného systému řízení budov. Využívá se grafické nadstavbové výbavy pro rychlou a včasnou orientaci v objektech a budovách. Tím se maximálně zkracuje doba začátku hašení od vyhlášení požáru. Ústředna má programovatelné výstupy a může těmito výstupy ovládat například protipožární dveře, hasicí zařízení, klíčové trezory aj (Hladík, 2011).

Normy Elektronické požární signalizace:

1) Zákon č. 133/1985 Sb. „O požární ochraně“,
2) ČSN 730875 „navrhování elektrické požární signalizace“
3) ČSN 342710 „předpisy pro zařízení EPS“ (Bartušek,2015).



Obrázek 3 – Systém EPS (Bartušek, 2015)

Systémy elektronické požární signalizace

V současné době se používají dva systémy EPS, a to:

1) s kolektivní adresací – ústředna umí určit místo požáru, ale nedokáže zjistit, z jakého konkrétního čidla byl požár detekován,
2) s individuální adresací – zde jsou použity systémy sériové a paralelní adresace, ústředna je schopna identifikovat stav jednotlivých hlásičů (Bartušek, 2015).

Ústředny elektronické požární signalizace

1) konvenční neadresované – propojení je proudové, po vyhlášení poplachu nelze zjistit, jaký hlásič poplach vyvolal, na jedné lince může být připojeno až 32 hlásičů,

2) konvenční adresné – hlásiče mají konkrétní adresu a podle adresy můžeme zjistit, který hlásič poplach vyvolal, z výroby jsou hlásiče nastaveny na stavy klid – poplach,
3) analogové – ústředna přijímá více stavové údaje pomocí algoritmů a rozhoduje se na tomto základě, jestli jde o normální stav, poruchu, předpoplach nebo poplach. Hlásiče v tomto systému mají vlastní adresu,
4) interaktivní – využití interaktivních hlásičů, které obsahují mikroprocesor a vyhodnocují okolní situace a vyhodnocené informace předávají ústředně. Hlásiče jsou adresné a odolné vůči negativním vlivům jako je elektromagnetická indukce (Bartušek, 2015).

Hlásiče elektronické požární signalizace

Hlásiče EPS pracují dle různých fyzikálních principů, a to na základě vyhodnocování optických, ionizačních nebo teplotních prostředí, ve kterých jsou umístěny (Bartušek, 2015).

Automatické požární hlásiče

Jsou to zařízení, které reagují předáním poplachové informace na průvodní jevy jako je kouř, nárůst teploty, plameny nebo jejich kombinace. Umístění se provádí na základě odpovídajících norem, předpisů výrobce a pokynů pro montáž a projekci (Bartušek,2015).

Rozdělení dle principu funkce:

1) hlásiče teplotní,
2) hlásiče kouře,
3) hlásiče ionizační,
4) hlásiče optické,
5) hlásiče tlakové,
6) hlásiče odporové,
7) hlásiče kombinované tzn. multisenzorové (Bartušek, 2015).

Manuální – tlačítkové

Tyto hlásiče jsou vždy červené barvy, umisťují se do výšky 140 cm od podlahy, a to u východů, aby byly snadno dosažitelně pro unikající osobu. Hlásiče slouží pro vyhlášení poplachu osobou, která registruje vznikající požár. Používají se pro neadresné a adresné

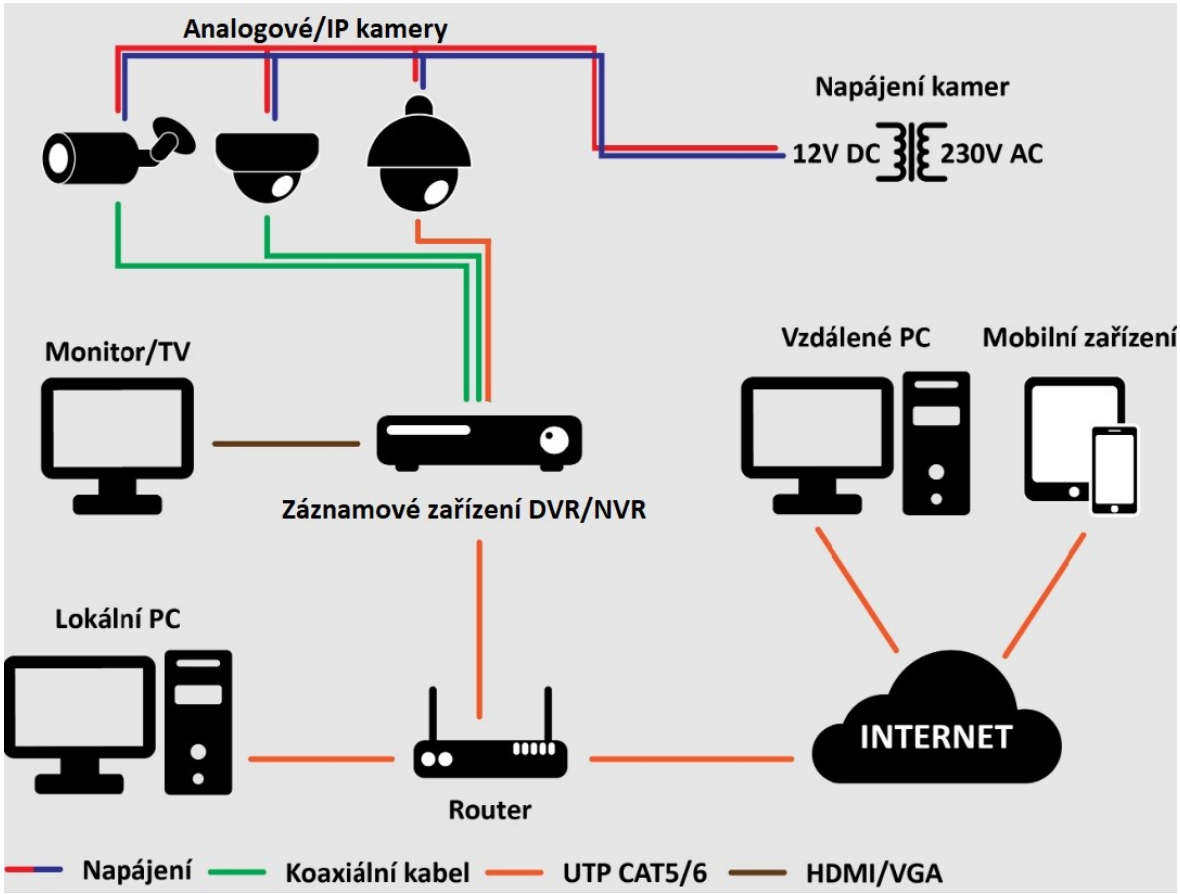
systémy a podle toho se volí, jestli je tlačítko s mikrospínačem, zakončovacím rezistorem nebo elektronikou (Bartušek, 2015).

1.4 Kamerové systémy

Cloused circuit Televison (dále jen „CCTV“) neboli uzavřený televizní okruh se rozděluje na tři základní typy, a to na:

1) analogové systémy,
2) hybridní systémy,
3) digitální systémy.

Každý z těchto typů má specifické vlastnosti a efektivita se různí tím, kde a jak jsou nasazeny. Mezi základní rozdíly řadíme způsoby zpracování signálu, kvalitu výstupního obrazu, inteligenci funkcí, přenosové trasy a také finanční náklady (Kameryskladem, 2020).



Obrázek 4 – CCTV možné schéma zapojení (Troch, upraveno)

Analogové systémy

Tento typ systému, který je určen pro monitorování a záznam obrazu, se řadí mezi ty nejstarší a většinou se nahrazuje novější technologií. U analogového systému probíhá přenos pomocí koaxiálního kabelu. Všechna obrazová data se zpracovávají až v záznamovém zařízení s označením DVR (Digital Video Recorder), zde probíhá také digitalizace obrazu.

Výhody: nízká pořizovací cena, žádné zpoždění obrazu.

Nevýhody: nižší kvalita obrazu oproti digitálním kamerám (Honey, 1999).

Hybridní systémy

Tyto systémy se využívají při modernizaci analogových systému. Výhodou je využití původní přenosové trasy. Signál je stále přenášen koaxiálním kabelem, ale kamery již mají vysoké rozlišení obrazu, až 4 K (Alarmtechnik, 2020).

Digitální systémy

Jedná se o systémy používající IP kamery, které zpracovávají pořízený obraz v rámci kamery, kdy směrem k uživateli nebo k záznamovému zařízení NVR (Network Video Recorder) jde už zpracovaný obrazový signál. Pro přenos dat se využívá kroucená dvoulinka, data lze přenášet i bezdrátově.

Výhody: vysoké rozlišení kamer, bezdrátový přenos.

Nevýhody: pořizovací náklady, větší náchylnost napadnutí kamery, kompatibilita různých výrobců (Kameryskladem, 2020).

Technologie kamer

Speciální technologie v podobě hardwaru či softwaru, které ovlivňují kvalitu záznamu.

1) WDR – kompenzuje velké světelné rozdíly (automatický jas),
2) NDR – digitální redukce šumu, tzn. *z*lepšuje výslednou kvalitu záznamu,
3) IR – infračervený přísvit, tzn. noční vidění (obraz je černobílý),
4) Krytí IP a IK – IP určuje míru odolnosti proti vlhkosti a vodě; IK určuje mechanickou odolnost (Microsegur; Delta; Tint; Redakce, 2021).

Inteligentní funkce

Těchto funkcí se využívá při automatizaci a zvýšení bezpečnosti v monitorované oblasti.

Mezi tyto funkce patří:

1) termální zobrazení,
2) počítání osob,
3) detekce a rozpoznání osob,
4) rozpoznání tváří,
5) rozpoznávání poznávacích značek,
6) hlídání předmětů,
7) audio-video konvergence – vysílání varovného signálu v reálném čase
8) detekce pohybu,
9) ochrana perimetru (Hikvision, 2023).

1.5 Mechanické zábranné systémy

Mechanické zábranné systémy (dále jen MZS) se považují za základní prvek ochrany objektů a osob v průmyslu komerční bezpečnosti. Veškeré mechanické prvky, které zabraňují násilnému vniknutí nepovolané osoby do střeženého objektu přes zóny oplocení nebo dveřními či okenními vstupy, případně osoby, které manipuluji s chráněnými předměty v zabezpečeném objektu, patří do MZS. MZS jsou tedy základním stavebním kamenem pro komplexní zabezpečení bytových i nebytových objektů (Lukáš, Ivanka, 2014).

Mezi mechanické zábranné prvky řadíme:

1) všechny zámkové systémy,
2) bezpečnostní kování,
3) pomocné zámkové a uzamykací, nebo zavírací systémy,
4) bezpečnostní dveře,
5) mechanické závory,
6) mříže, rolety,
7) bezpečnostní fólie,
8) vytvrzovaná bezpečnostní a sandwichová skla,
9) přenosné pokladny,

10) trezory a trezorové systémy,
11) bezpečnostní skříně,
12) speciální zavazadla cenin a peněz,
13) ruční bezpečnostní plomby,
14) mechanické prvky obvodového zabezpečení (Lukáš, Ivanka, 2014).

Podle pyramidy bezpečnosti se provádí certifikace výrobků MZS. Certifikaci a hodnocení výrobků provádí nezávislá laboratoř. Odolnost a požadavky proti vloupání se řídí normou ČSN EN 1627 (746001) (Lukáš, Ivanka, 2014).

Jak uvádí Ján Ivanka *„Pyramida bezpečnosti je jednotící komunikační prvek, který usnadňuje a zpřehledňuje identifikaci výrobků mechanických zábranných prostředků s ověřenou úrovní jakosti a je zaměřen výhradně na certifikované výrobky MZS.“* (Ivanka, 2014)

Obrázek 5 – Pyramida bezpečnosti (Šimíček, 2015)

Systémy MZS můžeme rozdělit do 4 základních skupin:

1) obvodová ochrana – pojímá nejširší pásmo a zajišťuje bezpečnost okolo objektu, který je chráněn. Obvod lze pak chápat jako přírodní umělé bariéry, jako jsou vodní toky, ploty, zdi aj.,

2) plášťová ochrana – neboli objektová ochrana, která chrání objekt před vniknutím. Jedná se zejména o zabezpečení oken, balkonů a dveří,
3) předmětová ochrana – jde o zabezpečení úschovných míst a prostorů před narušením nebo neoprávněnou manipulací. Mohou to být prostory pro úschovu cenných papírů, dokumentů, peněz aj.,
4) speciální ochrana – je chemická ochrana předmětů. Do této skupiny patří i ochrana označována jako „ostatní“, patří zde pečetě, plomby aj (Lukáš, Ivanka 2014).

2 UTAJOVANÉ INFORMACE

Informace a její definice má mnoho významů. Nejprostší vysvětlení je, že informace je sdělení určitého typu jako je zpráva, nebo přehled informací a znalostí, které se dají předat dál. Informace můžeme považovat za zřetelné zprávy, sdělení, vědomosti, znalosti, údaje, které jsme schopni zachytit, porozumět jim a dává nám zřetelný smysl. Tyto údaje mají souvislost, obsah, kvalitu, význam a pro adresáty mají hodnotu. Pro člověka je informace cenným zbožím, které může vlastnit (Barták, Bečvář a Bechyně et. al., 1999).

Pojem utajovaná informace je přesně daný pojem a je vymezen zákonem číslo 412/2005Sb. o ochraně utajovaných informací a o bezpečnosti způsobilosti. Zákon ji definuje, v § 2 písmene a) jako *„informaci v jakékoli podobě nebo zneužití může způsobit újmu zájmu České republiky nebo může být pro zájem nevýhodné. Tato informace je uvedena v seznamu utajovaných informací“ (*§ 139) (Česko, 2005).

Utajované informace jsou ty, které jsou zapsány v seznamu utajovaných informací. Národní bezpečnostní úřad zpracovává návrh tohoto seznamu. Vláda svým nařízením následně vydá seznam. Utajovaná informace musí plnit znaky formální i materiální. Formální znaky jsou určeny nařízením vlády. Tato informace musí obsahovat veškeré povinné znaky, pokud některých z těchto znaků nebude obsahovat, nejedná se o utajovanou informaci (Dvořák, Chrobák, 2018).

Formální, materiální znaky a újmy

Utajovaná informace musí sebou nést zřetelné znaky, aby mohla být za utajovanou informaci považována. Níže je uvedeno, jaké znaky a újmy může utajovaná informace mít.

Formální znaky – jak již bylo zmíněno, utajovaná informace musí obsahovat zřetelné znaky, aby to vůbec byla utajována informace. Formální znaky rozdělujeme do tří skupin:

1) utajovaná informace musí být zaznamenána. Dočteme se v zákoně, že informace má být zaznamenána na jakýkoli nosič a jakýmkoli způsobem, záleží to především na pořizovateli utajované informace (Dvořák, Chrobák, 2018),
2) utajovaná informace musí být řádně označena dle zákona 412/2005 Sb., o ochraně utajovaných informací. V tomto případě ale zákon neurčuje, jak danou informaci označit, obsahuje pouze § 4, kde určuje stupně utajení. Vyznačení údajů na utajovanou informaci, evidenci a vyznačení stupně utajení upravují tyto dva paragrafy §21 a §22 (Dvořák, Chrobák, 2018; Česko, 2005),

3) utajovanou informaci je nutno zapsat do seznamu utajovaných informací. Zákon 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, který obsahuje paragraf § 139 říká, že Národní bezpečnostní úřad má v gesci zpracovávání návrhu na seznam utajovaných informací, následně vláda vydá soupis utajovaných informací v podobě vlastního nařízení. Od 1.1. 2006 je účinné nařízení vlády č. 522/2005 Sb., kterým se stanovuje seznam pro utajované informace, kde každá utajovaná informace je klasifikována do skupin jednotlivých úřadů, kterých se to týká a do stupňů utajení nebo jejich rozsahu (Dvořák, Chrobák, 2018; Česko, 2005).

Stupně utajení

Zákon č. 412/2005 Sb. v §4. vymezuje stupně utajení a utajovaná informace je pod tímto stupněm zapsána v seznamu utajovaných informací. Klasifikace stupně se určuje tím, jakou újmu by mohlo vyzrazení informace způsobit České republice.

Dělení stupně utajení:

1) vyhrazené – jde o nejmenší riziko ze všech stupňů, její vyzrazení může mít za následek znevýhodnění zájmů České republiky,
2) důvěrné – jde o závažnější riziko, které může mít pro Českou republiku prostou újmu na jejich zájmech,
3) tajné – vyzrazení nebo zneužití informace při tomto stupni by znamenalo pro Českou republiku vážnou újmu na jejich zájmech,
4) přísně tajné – vyzrazení nebo zneužití informace u tohoto stupně je nejpřísněji trestáno a jedná se o mimořádnou újmu pro Českou republiku (Česko, 2005).

Materiální znaky

Mezi tyto znaky se řadí skutečnost, že újma zájmu nebo nevýhodnost pro Českou republiku může vzniknout zneužitím nebo vyzrazením utajované informace (Dvořák, Chrobák, 2018; Česko 2005).

Újmy zájmu pro Českou republiku

Zákon č. 412/2005 Sb. v §3 (1) říká že:

„Újmou zájmu České republiky se pro účely tohoto zákona rozumí poškození nebo ohrožení zájmu České republiky, podle závažnosti poškození nebo ohrožení zájmu České republiky se újma člení na mimořádně závažnou újmu, vážnou újmu a prostou újmu.“ (Česko, 2005)

Zákon č. 412/2005 Sb. §3 (2) říká že:

„Mimořádně vážná újma zájmu České republiky vznikne vyzrazením utajované informace neoprávněné osobě nebo zneužitím utajované informace, které může mít za následek

a) bezprostřední ohrožení svrchovanosti, územní celistvosti nebo demokratických základů České republiky,

b) rozsáhlé ztráty na lidských životech nebo rozsáhlé ohrožení zdraví obyvatel,

c) mimořádně vážné nebo dlouhodobé poškození ekonomiky České republiky,

d) značné narušení vnitřního pořádku a bezpečnosti České republiky,

e) mimořádně vážné ohrožení významných bezpečnostních operací nebo činnosti zpravodajských služeb,

f) mimořádně vážné ohrožení činnosti Organizace Severoatlantické smlouvy, Evropské unie nebo členského státu,

g) mimořádně vážné ohrožení bojeschopnosti ozbrojených sil České republiky, Organizace Severoatlantické smlouvy nebo jiného členského státu nebo členského státu Evropské unie, nebo

h) mimořádně vážné poškození diplomatických nebo jiných vztahů České republiky k Organizaci Severoatlantické smlouvy, Evropské unii nebo členskému státu.“ (Česko, 2005)

zákon č. 412/2005 Sb. §3 (3) říká že:

„Vážná újma zájmu České republiky vznikne vyzrazením utajované informace neoprávněné osobě nebo zneužitím utajované informace, které může mít za následek

a) ohrožení svrchovanosti, územní celistvosti a demokratických základů České republiky,

b) značnou škodu České republiky ve finanční, měnové, nebo hospodářské oblasti,

c) ztráty na lidských životech nebo ohrožení zdraví obyvatel,

d) narušení vnitřního pořádku a bezpečnosti České republiky,

e) vážné ohrožení bojeschopnosti ozbrojených sil České republiky, Organizace Severoatlantické smlouvy nebo jiného členského státu nebo členského státu Evropské unie,

f) vážné ohrožení významných bezpečnostních operací nebo činnosti zpravodajských služeb,

g) vážné ohrožení činnosti Organizace Severoatlantické smlouvy, Evropské unie, nebo členského státu,

h) vážné narušení diplomatických vztahů České republiky k Organizaci Severoatlantické smlouvy, Evropské unii nebo členského státu nebo jiného státu, nebo

i) vážné zvýšení mezinárodního napětí.“ (Česko, 2005)

Zákon č. 412/2005 Sb. §3 (4) říká že:

„Prostá újma zájmu České republiky vznikne vyzrazením utajované informace neoprávněné osobě nebo zneužitím utajované informace, které může mít za následek

a) zhoršení vztahů České republiky s cizí mocí,

b) ohrožení bezpečnosti jednotlivce,

c) ohrožení bojeschopnosti ozbrojených sil České republiky, Organizace Severoatlantické smlouvy nebo jejího členského státu nebo členského státu Evropské unie,

d) ohrožení bezpečnostních operací nebo činnosti zpravodajských služeb,

e) ohrožení činnosti Organizace Severoatlantické smlouvy, Evropské unie nebo jejich členského státu,

f) zmaření, ztížení anebo ohrožení prověřování nebo vyšetřování zvlášť závažných zločinů nebo usnadnění jejich páchání,

g) vznik nezanedbatelné škody České republice, nebo

h) závažné narušení ekonomických zájmů České republiky.“ (Česko, 2005)

3 BEZPEČNOST

V dnešní době se pojem bezpečnost skloňuje všemi pády, ať už jde o vnitřní, vnější bezpečnost, informační bezpečnost a mnoho dalších bezpečností, jedno mají ovšem stejné, a to, že jsou závislé na čase a vývoji společnosti. Definic pro bezpečnost je mnoho, ale v mezinárodní bezpečnosti a v jeho tradičním pojetí je sledována takřka výhradně vojenská bezpečnost. Ta stále patří mezi ty nejdůležitější, avšak velkou váhu mají i problémy ekonomické, enviromentální, společenské a politické (Lukáš 2012; Sheehan, 2005).

Nevládními aktéry, kteří se zapojují do mezinárodního bezpečnostního dění, mohou být transnacionální média, reprezentace národů bez státu a různé nevládní bezpečnostní organizace. V hybridních bezpečnostních organizacích mohou konfigurovat i vládní a nevládní představitelé mezinárodních bezpečnostních organizacích (Lukáš 2012; Kegley, Wittkopf, 2006).

Informační bezpečnost

Informační bezpečnost patří mezi důležité druhy bezpečnosti. K největšímu rozvoji došlo s rozvojem počítačových sítí v 70. letech minulého století. Oblast šifrování už se prováděla o mnoho dříve. Hlavním cílem informační bezpečnosti je zabezpečit informace proti neoprávněnému přístupu vůči jejich úpravě nebo zničení. Počítače, počítačové sítě a informační technologie patří na vysokou úroveň. I informační bezpečnost se řadí v dnešní době na velmi vysokou úroveň. Procesně se od jiných bezpečností neliší, jejím výstupem zabezpečení je projekt a jeho realizace. Odlišné je prostředí, kde se zajišťuje bezpečnost. Typů útoků, které se uskutečňují na informační technologie, je řada, využívá se slabin v systému, aplikačních softwarových vybaveních a v prvcích počítačových sítí. Algoritmy a data jsou informační technologie, jejich kvalita je skloubena s matematizací, proto je práce v této oblasti spjata s tvořivostí a s velkou porcí znalostí (Lukáš, Jašek 2015).

4 PERSONÁLNÍ BEZPEČNOST

Personální bezpečnost je řazena mezi základní druhy bezpečnosti. Je využívána pro zajištění ochrany utajovaných informací. Jedná se vlastně o seznam osob, které mohou mít přístup k utajovaným informacím, aby taková osoba měla přístup k utajovaným informacím musí dodržet zákonem vymezené podmínky (Dvořák, Chrobák, 2018).

Primárním cílem personální bezpečnosti je zajištění toho, aby měla přístup k utajovaným informacím jen ta fyzická osoba, která na ni má, nebo může mít nárok a potřebuje toto povolení ke své pracovní činnosti. Tato osoba potřebuje mít potřebné oprávnění od Národního bezpečnostního úřadu, po udělení tohoto oprávnění podléhá tato osoba své odpovědné osobě, ta potom ručí každoročně za to, že je jeho podřízená osoba proškolena a zapisuje o proškolení záznamy. Pod proškolením se ukrývá spousta opatření k eliminaci nebezpečí, které vedou například k selhání lidského faktoru. Personální bezpečnost taktéž zabezpečuje ochranu osob, které přijdou do styku s citlivými informacemi (Rodryčová, Staša, 2000).

Fyzické osoby, jež potřebují pracovat s utajovanými informacemi, musí splňovat kritéria stanovená zákonem a musí se podrobit prověrce. Každý ze čtyř stupňů utajení má tato kritéria pro udělení jiná. Různé podmínky jsou jak u udělení stupně Vyhrazené, tak u dalších stupňů - Důvěrné, Tajné, Přísně tajné. Podle toho, do jaké skupiny utajení osoba spadá, je určen i rozsah a způsob prověření. Pro stupeň Vyhrazené se vydává osvědčení fyzické osoby a u dalších stupňů už je to osvědčení pro tuto fyzickou osobu. Níže uvedena tabulka s podmínkami. (NBÚ)

Tabulka 1 – podmínky pro udělení stupně utajení (NBÚ)

Podmínky	**VYHRAZENÉ (oznámení)**	**DŮVĚRNÉ, TAJNÉ, PŘÍSNĚ TAJNÉ (osvědčení)**
Svéprávnost	ANO	ANO
Věk minimálně 18 let	ANO	ANO
Bezúhonnost	ANO	ANO
Státní občanství ČR, země EU a NATO	NE	ANO
Osobnostní způsobilost	NE	ANO
Bezpečnostní spolehlivost	NE	ANO

Výše uvedená tabulka uvádí pouze základní parametry, které osoba, co žádá o udělení jednoho ze čtyř stupňů, musí splnit. Například u stupně Vyhrazené kontroluje všechny náležitosti osoba odpovědná, která je přidělena osobě žádající. Prověrky, které je daleko podrobnější, se provádí u stupňů Důvěrné, Tajné, Přísně tajné. Prověrka se taktéž nazývá bezpečnostní řízení. Tato bezpečnostní řízení uskutečňuje na základě žádosti Národní bezpečnostní úřad, dále zpravodajské služby a Ministerstvo vnitra, vždy se jedná o opodstatněné žádosti pro vyprané příslušníky, uchazeče (NBÚ).

5 ADMINISTRATIVNÍ BEZPEČNOST

Mezi další základní druhy bezpečnosti se řadí administrativní bezpečnost, ta taktéž zajišťuje ochranu utajovaných informací. Administrativní bezpečnost podléhá zákonu 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, dále vyhlášce 275/2022 Sb., o administrativní bezpečnosti a o registrech utajovaných informací. Administrativní bezpečnost se uplatňuje při kterékoliv práci s utajovanými informacemi. Například:

1) tvorbě,
2) příjmu,
3) evidenci,
4) zpracování odesílání,
5) přepravě,
6) přenášení,
7) ukládání,
8) archivaci,
9) skartaci a jiném nakládání s utajovanými informacemi (NBÚ; Česko, 2022).

Při administrativní bezpečnosti se dodržují určitá pravidla, která se musí při zacházení s utajovanými informacemi dodržovat. Jde zejména o hmotný nosič, který obsahuje utajovanou informaci. Utajovaná informace se musí řádně označit, evidovat, přenášet, ukládat, předávat a řádně musí probíhat i zánik a zničení nosiče. Mezi druhy nosičů informace patří:

1) nosiče obrazové,
2) nosiče zvukové,
3) nosiče listinné,
4) nosiče elektronické (Dvořák, Chrobák, 2018).

Nosič musí být důkladně poznačen stanovenými určenými informacemi. Zejména jde o tyto informace:

1) název původce utajované informace,
2) stupeň utajení,
3) číslo jednací,
4) datum vzniku utajované informace (Dvořák, Chrobák, 2018; Česko, 2005).

Vyhláška č. 529/2005 Sb., stanovuje používání administrativních pomůcek při jakékoli manipulaci s utajovanými informacemi. Administrativní pomůcky jsou tyto:

1) jednací a pomocné jednací protokoly,
2) manipulační, doručovací, zápůjční knihy,
3) kontrolní listy,
4) sběrné archy apod.

Všechny tyto pomůcky se evidují a jejich evidenci má na starosti pověřená osoba, která s nimi musí nakládat postupem, který zajistí jejich ochranu proti zneužití nebo ztrátě (Česko, 2005).

Název orgánu státu
(Organizační celek)
nebo právnické osoby
anebo jméno, příjmení a sídlo podnikající fyzické osoby

STUPEŇ UTAJENÍ
UTAJOVANÉHO DOKUMENTU/SPISU*)

KONTROLNÍ LIST UTAJOVANÉHO DOKUMENTU/SPISU*)

Věc:

č. j./značka spisu*) ....

....

....

SEZNÁMENÍ S OBSAHEM UTAJOVANÉHO DOKUMENTU/SPISU*)

POŘ. ČÍSLO	DATUM	JMÉNO A PŘÍJMENÍ	PODPIS	POZNÁMKA

Na předepsané pole v prvním řádku vypište číslo jednací utajovaného dokumentu nebo spisovou značku spisu, ke kterému je kontrolní list připojen. Je-li kontrolní list vyhotoven osobou, která se s obsahem utajovaného dokumentu seznámila jako první ještě před zaevidováním utajovaného dokumentu, uvede se číslo jednací utajovaného dokumentu odesílatele. Při změně čísla jednacího utajovaného dokumentu původní zápis přeškrtněte tak, aby zůstal čitelný a na následující pole v řádku vypište nové číslo jednací utajovaného dokumentu.

*) Nehodící se škrtněte.

Obrázek 6 – kontrolní list (Česko, 2022)

Příloha č. 8 k vyhlášce č. 275/2022 Sb.

Vzor úpravy přední strany prvního listu utajovaného dokumentu

STUPEŇ UTAJENÍ
UTAJOVAT DO:

Název orgánu státu
nebo právnické osoby anebo
jméno, příjmení a sídlo
podnikající fyzické osoby

Datum, případně místo vzniku

Č. j.:

Výtisk č. (Výtisk jediný)
Počet listů:
Rozdělovník přiložen
Přílohy utajované:
Přílohy neutajované:

……..
.....obsah……
……

STUPEŇ UTAJENÍ
číslo listu nebo stránky

Slova „UTAJOVAT DO“ se uvedou, pouze pokud charakter utajované informace vyžaduje, aby byla omezena doba, po kterou bude informace utajována podle § 22 odst. 3 zákona.
Údaje o přílohách se uvádí pouze, pokud utajovaný dokument přílohy obsahuje.
Umístění čísla listu nebo stránky nemusí být uprostřed.
Slova „Rozdělovník přiložen“ se uvádí v případě, kdy je rozdělovník vyhotoven na samostatném listu. Umístění textu nemusí odpovídat vzoru.

Obrázek 7 – první list utajovaného dokumentu

(Česko, 2005)

6 FYZICKÁ BEZPEČNOST

Fyzická bezpečnost je definována hlavou V. zákona 412/2005Sb. a vyhláškou Národního bezpečnostního úřadu č. 528/2005 Sb., kde se fyzická bezpečnost zaobírá ochranou prostoru, ve kterých se utajované informace projednávají, uchovávají nebo vznikají. Jsou stanovena pravidla technického a režimového charakteru, která se pojí s vybraným prostorem. Hlavním cílem fyzické bezpečnosti je zabránit fyzické osobě, která nemá povolení ke vstupu do prostoru, kde jsou utajované informace, nebo se s nimi nakládá, případně ji ztížit tento pokus a zaznamenat jej a ve výsledku tak zabránit buď zcizení, poškození nebo jakémukoli jinému způsobu ohrožení utajované informace (Kloboučková, 2015).

Objekt

Za objekt se považuje budova nebo jiný ohraničený prostor, ve kterém se obvykle nachází oblasti zabezpečené nebo jednací. Technické prostředky určené do těchto oblastí se určují pomocí vyhlášky Národního bezpečnostního úřadu, který stanoví míru zabezpečení (Kloboučková, 2015).

Zabezpečená oblast

Zabezpečená oblast je ohraničený prostor v konkrétním objektu. Zabezpečovaná oblast se zabezpečuje na základě daných kritérií v závislosti na vyhodnocení rizik a na tom, do jaké kategorie, třídy patří. Podle nejvyššího stupně utajení utajovaných informací se určí míra zabezpečených oblastí. Jsou zařazeny do kategorií vyhrazené, důvěrné, tajné, přísně tajné. Třídy zabezpečených oblastí:

1) se vstupem do oblasti dojde k seznámení s utajovanými informacemi,
2) se vstupem do oblasti nedochází k seznámení s utajovanou informací (Kloboučková, 2015).

Jednací oblast

Jednací oblast je zabezpečená oblast definována jako uzavřený prostor v objektu. Projednávání utajovaných informací se stupněm tajné a přísně tajné jsou projednávána výhradně v jednací místnosti. Celkový rozsah použití fyzické bezpečnosti v jednací místnosti se odvíjí od stupně utajení utajované informace. Odpovědná osoba pak zajistí, aby nedošlo, nebo nedocházelo k odcizení nebo zneužití těchto utajovaných informací. Dále odpovědná osob odpovídá za podání žádosti Národnímu bezpečnostnímu úřad o provedení kontroly, zpravidla to bývá v součinnosti s policií České republiky a zpravodajskou službou,

které tyto služby provádí u třetích subjektů. Provedení kontroly se týká prověření toho, zda nedochází v jednací místnosti k nedovolenému použití technických prostředků za účelem získání utajované informace (Kloboučková, 2015).

Opatření fyzické bezpečnosti

Mezi tato opatření patří:

1) ostraha – zřizuje se u objektů, kde se nachází zabezpečená oblast, nebo jednací oblast v závislosti na určené kategorii utajovaných informací. Ostraha se zřizuje buď nepřetržitá nebo technickým prostředkem (poplachové hlášení), který umožní rychlý zásah,
2) režimová opatření – je to soubor opatření, který stanoví oprávnění osob a dopravních prostředků pro vstup. Pro vstup je nutné mít oznámení o splnění podmínek pro přístup k utajované informaci (platí pro stupeň vyhrazené), nebo osvědčení pro vyšší stupeň kategorie. Ostatní osoby mohou být vpuštěny za podmínek uvedených ve vyhlášce č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, věnující se režimu pohybu osob a dopravních prostředků (Kloboučková,2015).

Technické prostředky

Zákon č. 412/2005 stanoví § 30 výčet technických prostředků k odrazení, nebo zabránění přístupu k utajované informaci či k jejímu včasnému odhalení. Jde zejména o tyto prostředky:

1) mechanické zábranné prostředky,
2) elektronická zařízení se systémem kontroly vstupu,
3) speciální televizní systémy,
4) zařízení fyzického ničení nosičů informací,
5) zařízení proti pasivnímu či aktivnímu odposlechu aj (Kloboučková, 2015).

Bezpečnost informačních systémů

Bezpečnost informačních systému se věnuje otázkám spojených s existencí utajované informace v informačních systémech a jejich předávání. Využívání počítačových systému raketově roste a je potřeba věnovat ochraně těchto systému velkou pozornost. Informační systém nakládající s utajovanými informacemi dle definice v zákoně č. 412/2005 Sb. říká:

„jeden nebo více počítačů, jejich programové vybavení a k tomu patřící periferní zařízení, taktéž správa tohoto informačního systému a k tomuto systému se vztahující procesy nebo prostředky schopně provádět sběr, tvorbu, zpracování, ukládání, zobrazení nebo přenos utajovaných informací.“ (Česko, 2005)

Informační systém je tedy brán nejen jako počítač a jeho programové vybavení apod., ale také pro jeho schopnost sběru, tvorby, zpracování, ukládání, zobrazení nebo pro jeho schopnost přenosu utajovaných informací. Bezpečnosti informačního systému můžeme dosáhnout s tímto souborem opatření z oblasti:

1) počítačové a komunikační bezpečnosti,
2) kryptografické ochrany,
3) ochrany proti úniku kompromitujícího vyzařování,
4) administrativní bezpečnosti a organizačních opatření,
5) personální bezpečnosti,
6) fyzické bezpečnosti informačního systému (Kloboučková, 2015).

Více o této problematice se můžeme dozvědět ve vyhlášce NBÚ č. 523/2011 Sb. o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor ve znění pozdějších předpisů.

7 ANALÝZA RIZIK

Analýzou rizik se rozumí posouzení nebezpečí či odhalování chyb v již aplikovaném procesu nebo systému. Metody Brainstormingu a analýzy Failure Mode and Effect Analysis (dále jen FMEA) v českém překladu analýza možný vad a následků, budou využity pro záměry bakalářské práce. Jejich využití jsou popsána a vysvětlena níže v této kapitole (Grasseová, Dubec a Řehák, 2012).

Brainstorming

Technika Brainstormingu je kreativní, tvůrčí metoda založena na tvorbě nápadů a využití potenciálu skupiny osob. Záměrem metody je produkce těch nejlepších nápadů, myšlenek v co nejkratším časovém úseku od osob, které jsou k této metodě přizvány. Účastnící Brainstormingu prochází třemi fázemi s určenými pravidly. Brainstorming rozdělujeme na fáze:

1) první fáze je nazývána přípravou fází a určí se zde téma, účastníci metody a počet účastníků. Ze skupiny se vybere jeden zapisovatel a moderátor sezení. Moderátor hlídá dodržování pravidel a řídí celé sezení. Zapisoval má za úkol zapisování veškerých nápadů a myšlenek. Zápisky musí být viditelné pro všechny zúčastněné, aby se jimi mohli dále inspirovat,
2) druhá fáze je realizační fází. U této fáze všichni zúčastnění sdělují své názory spontánně nebo jak určí moderátor, ten vždy před zahájením sezení zopakuje pravidla a téma. Zapisovatel zapisuje slova doslovně,
3) poslední fázi je zhodnocení a využití zapsaných výsledků. Hodnotí se podobné, nebo stejné nápady, které se pak shromáždí do větších skupin. Hodnocení může probíhat více způsoby (Grasseová, Dubec a Řehák, 2012).

Pravidla Brainstormingu:

1) první pravidlo – nikdo nesmí být kritizován za to, co ho napadne v průběhu sezení,
2) druhé pravidlo – vyhodnocení výsledku probíhá až v poslední fázi sezení,
3) třetí pravidlo – každý zúčastněný by měl říci myšlenku, která ho napadne. U této metody platí, čím víc myšlenek a nápadů, tím líp.

Na pravidla při Brainstormingu dohlíží moderátor sezení (Grasseová, Dubec a Řehák, 2012).

Analýza možných vad a následků

Analýza FMEA identifikuje možný vznik vad v určitém systému. Cílem je minimalizace budoucích ztrát. Metoda FMEA se aplikuje v řadě odvětví, jako je například řízení bezpečnosti. Pro analýzu FMEA je typické sestavení tabulky, kdy v jedné části máme uvedené možné příčiny poruch, jejich následek a v další části máme navržená doporučená opatření, pro snížení poruchy na co nejmenší míru, nebo úplné odstranění. Důležité je výsledné rizikové číslo, které autoři a vedení objektu akceptují nebo ne. Metoda se takto může opakovat několikrát za sebou s novými návrhy řešení, až je pro autory a vedení objektu výsledné rizikové číslo doporučeného opatření akceptovatelné (Dean H. Stamatis, 2019).

Abychom mohli aplikovat metodu FMEA je nutné začít tím, co se bude analyzovat, kdo bude v týmu odborníků, kteří následně sestaví seznam možných problému a vad, které mohou nastat. K zjištění možných vad a problému lze využít metodu Brainstormingu, která se uplatní i pro účely bakalářské práce. Do předem připraveného formuláře FMEA se zapíší všechny nápady vad a problémů, které vznikli při Brainstormingu, následně tým odborníků určí následek problému, jeho možný vznik a doplní se stávající opatření a stávající řízení procesu, dále se do doplněného formuláře doplní koeficienty na základě stanovených kritérií.

Do tabulky FMEA se vyplňují tři koeficienty a jsou to tyto:

1) význam vady – číselná hodnota vyjadřující závažnost důsledku chyby na celý systém. Hodnotí se podle významu vady,
2) výskyt vady – číselná hodnota vyjadřující pravděpodobnost výskytu vady v celém systému,
3) odhalení vady – číselná hodnota pro pravděpodobnost odhalení vady v celém systému, nebo také neodhalení vady.

Po vyplnění všech koeficientů se všechny tyto koeficienty mezi sebou na řádku vynásobí a výsledkem tohoto násobení je rizikové číslo. Rizikové číslo je údaj, který stanoví míru daného problému nebo vady (Dean H. Stamatis, 2019).

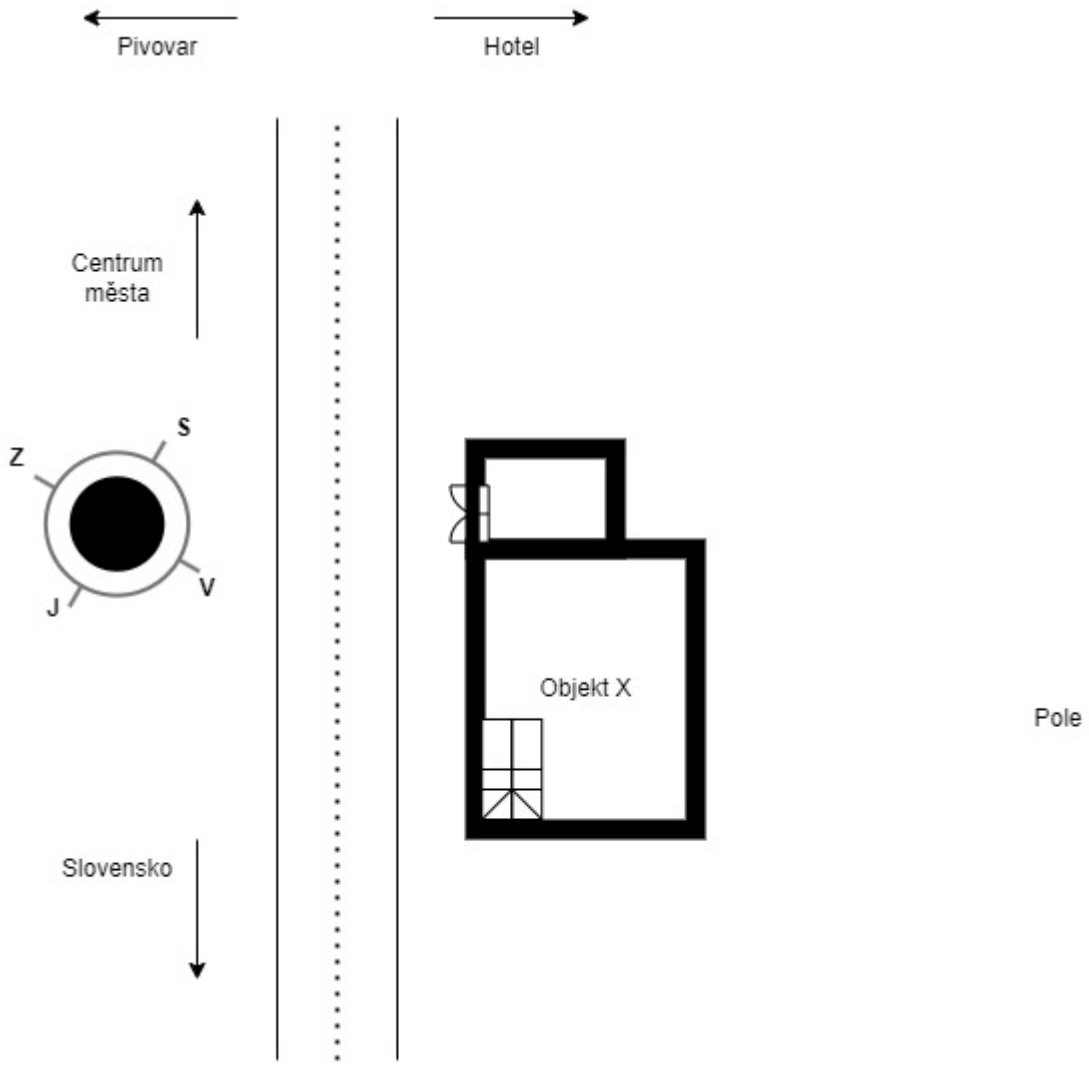
Tabulky koeficientů a jejich význam bude popsán v praktické části bakalářské práce.

II. PRAKTICKÁ ČÁST

8 POPIS OBJEKTU X

Pro praktickou část bakalářské práce se zvolil objekt X, který vlastní nejmenovaná státní instituce. Vybraná státní instituce nakládá s běžnými dokumenty a nyní má přejít k práci s utajovanými informacemi, které podléhají právním předpisům. Konkrétně se bude jednat o uložení a nakládání s utajovanými informacemi ve stupni Vyhrazené a Důvěrné. Objekt se nachází v Jihomoravském kraji ve středně velkém městě u hranic se Slovenskem. Jedná se o samostatný objekt umístěný v průmyslové zóně města. V blízkosti objektu je hotel a místní pivovar. Budova je vzdálena od centra města přibližně 15 minut pěšky. Za stejný časový úsek bychom přešli do sousedního státu. Přední část budovy je lemovaná chodníkem a pozemní komunikací, která je hlavní dopravní tepnou na Slovensko. Budova má půdorys obdélníku s přístavkem vstupní haly, kde je umístěna recepce s pracovníkem ostrahy. Projde-li se dveřmi naproti recepce, dostaneme se na chodbu, která vede kolem kanceláře ostrahy, jejich šatny, technické místnosti. Naproti této místnosti se nachází zasedací místnost, která sousedí s kuchyní a toalety. Dále po chodbě se dostaneme do 2. nadzemního podlaží a tam jsou prostory kanceláří, toalet a dvou místností, které mají sloužit k účelům zacházení s utajovanými informacemi. Jedna kancelář bude sloužit pro stupeň „DŮVĚRNÉ“ a další pro stupeň „VYHRAZENÉ“. V budově jsou pořízeny věci, jako jsou kancelářský nábytek, počítačové sestavy, tiskárny. Do nově zařizovaných prostor budou nově pořízeny multifunkční tiskárny, trezory a skartační přístroje. Nově bude budova pracovat v režimu dle:

1) zákona č. 412/ 2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti a vyhlášek,
2) vyhlášky NBÚ č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů,
3) vyhlášky č. 275/2022 Sb., o administrativní bezpečnosti a o registrech utajovaných informací.
4) normou ČSN EN 1627 (746001) s katalogovým kódem 514152 – dveře, okna, lehké obvodové pláště, mříže a okenice – odolnost proti vloupání – požadavky a klasifikace.



Obrázek 8 – Umístění objektu X (Autor vlastní, vytvořeno v programu draw.io)

8.1 Popis personální bezpečnosti

Pro udělení osvědčení na stupeň utajení Důvěrné musí všichni pracovníci splňovat podmínky dle zákona č. 412/2005 Sb. o ochraně utajovaných informací a bezpečnostní způsobilosti. Za zajištění udělení osvědčení zodpovídá ředitel instituce, který má za úkol zajišťovat termíny školení a následné proškolení zaměstnanců s právními předpisy v oblasti utajovaných informací. Tato školení jsou nutná ještě před tím, než se začnou pracovníci seznamovat s utajovanými informacemi. Ředitel instituce dále zajišťuje seznamování jen s těmi utajovanými informacemi, které zaměstnanci potřebují výhradně k výkonu práce. Přístup k těmto informacím se řídí podstatou nezbytnosti. Osoby, které mají oprávnění přístupu k utajovaným informacím, včetně stupně utajení, jsou vedeny ve vytvořeném seznamu a ten je uložen na příslušeném místě sekretariátu objektu.

8.2 Popis administrativní bezpečnosti

V objektu X se nově bude manipulovat s utajovanými informacemi se stupněm utajení Vyhrazené a Důvěrné. Při vzniku budoucí utajované informace se s ohledem, jak a moc mohou utajované informace způsobit škodu České republice, stanoví stupeň utajení. Klasifikaci stupně utajení a podrobnější informace, která sebou budoucí utajovaná informace nese, říká vyhláška č. 275/2022 Sb., o administrativní bezpečnosti a o registrech utajovaných informací. Evidování všech utajovaných informací má za úkol správce protokolu, který je eviduje v náležejících jednacích protokolech.

Do objektu budou pořízeny čtyři kusy počítačů, které budou umístěny v nově určených místnostech pro zpracování tajných informací do stupně Důvěrné. Na těchto počítačích budou naistalovány certifikované systémy, které následně umožní výše uvedené. Do tohoto systému budou mít přístup jen osoby pod vlastním uživatelským jménem a budou zodpovědní za zpracování utajovaných informací pouze do stupně utajení Důvěrné. Přístup budou mít pouze ti zaměstnanci, kteří mají ke svému výkonu práce patřičné osvědčení. Tisknout, nebo kopírovat lze jen v místnostech pro nakládání s utajovanými informacemi.

Dále budou používána nosná média, na která jdou nahrát utajované informace. Tato média musí být řádně označena a zaevidována na daného pracovníka, který s tímto médiem nakládá. Mohou být používána jen na certifikovaných systémech. Opis, překlad nebo výpis dokumentu je možný jen za předpokladu schválení ředitelem objektu.

V místnostech pro nakládání s utajovanými informacemi se budou instalovat trezory pro ukládání těchto informací dle určeného stupně utajení. Tyto místnosti budou mimo pracovní dobu uzamčeny a zabezpečeny zabezpečovacím systémem. Klíče k těmto místnostem jsou umístěny v kanceláři ostrahy. Tyto klíče lze proti podpisu oprávněné osoby vydat. O vydávání a příjem klíčů se stará ostraha. Ztráta nebo odcizení klíčů od těchto místností musí neprodleně hlásit řediteli objektu, který zajistí bezpečný přesun utajovaných informací do nově určené místnosti nebo objektu.

Přeprava utajovaných informací je možná pouze kurýrní službou, a to s dvojí ochranou pomocí obálek. První je obálka s odesílatelem, která obsahuje razítko, adresu příjemce a způsob doručení pomocí kurýra se slovy „Otevře pouze příjemce“. Druhá obálka je ta, kterou vlastní kurýr a je uzamykatelná. Kurýr pak následně převezme zásilku proti podpisu, musí mít osvědčení pro nakládání s utajovanými informacemi pro stupeň Důvěrné a převáží zásilku ve vozidlech určených státem.

8.3 Popis fyzické bezpečnosti

Objekt, se kterým pracujeme v této bakalářské práci, se nachází v jihomoravském kraji nejmenovaného města. Za chod objektu a jeho správu zodpovídá do této funkce jmenovaný ředitel, jenž odpovídá i za ochranu utajovaných informací. Dvoupatrová budova je postavena z cihel s tloušťkou obvodových stěn o síle 44 centimetrů. K zabezpečení objektu dopomáhá opatření fyzické bezpečnosti, to je kombinace ostrahy, technických prostředků a režimových opatření.

Ostraha

Objekt X byl do chvíle, než se změnil charakter práce z obyčejné administrativní budovy na budovu, která zachází s utajovanými informacemi, střežen pracovníkem instituce po dobu 8,5 hodiny. Aktuálně budova pracuje v režimu s nepřetržitou ostrahou, kdy je vždy jeden pracovník ostrahy instituce na svém stanovišti v kanceláři ostrahy a dohlíží na celý objekt. Střídání směn probíhá po 12 hodinách. Ostraha objektu X nemá za úkol provádět obchůzky kolem objektu, nýbrž plní úkoly ostrahy. Ty by měly být následující:

1) kontrola neoprávněných vstupů, funkčnost technických prostředků,,
2) vedení záznamů o závadách technických prostředků, které se neodkladně nahlásí řediteli,
3) činnosti spojené s výdejem a příjmem přidělených klíčů od budovy.

Režimová opatření

Z důvodu změny charakteru budovy bylo nutno pořídit elektronickou kontrolu vstupů (EKV). Pořízení tohoto systému vede k větší kontrole a povědomí o tom, kdo, kde a kam se pohybuje a za jakým účelem. Ředitel určuje osoby, které budou nebo nebudou mít přístup do jednotlivých prostor. V praxi to funguje tak, že se jména zaměstnanců nahrají do systému, určí se místnosti, které uživatel nově vydané identifikační karty může navštěvovat. Zaměstnanci tak mají přístupy určené podle funkce, kterou zastávají v instituci, jde vždy tak o nezbytně nutné přístupy k výkonu práce. To znamená, že ne všichni zaměstnanci mají přístup do prostor, kde se nakládá s utajovanými informacemi. Osoby, jež nemají přidělen žádný přístup do prostor objektu, jsou brány jako „návštěvníci objektu“ a vstup je tak povolen pouze s doprovodem ve formě místního zaměstnance instituce. Všichni zaměstnanci instituce musí při odchodu ze své kanceláře uzavřít všechny okna, vypnout elektrická zařízení a zamknout. Práce přes určenou pracovní dobu se vždy musí nahlásit pracovníkům ostrahy. Pracovní doma v této instituci je určena od 7:30 ranních do 16 hodin odpoledních.

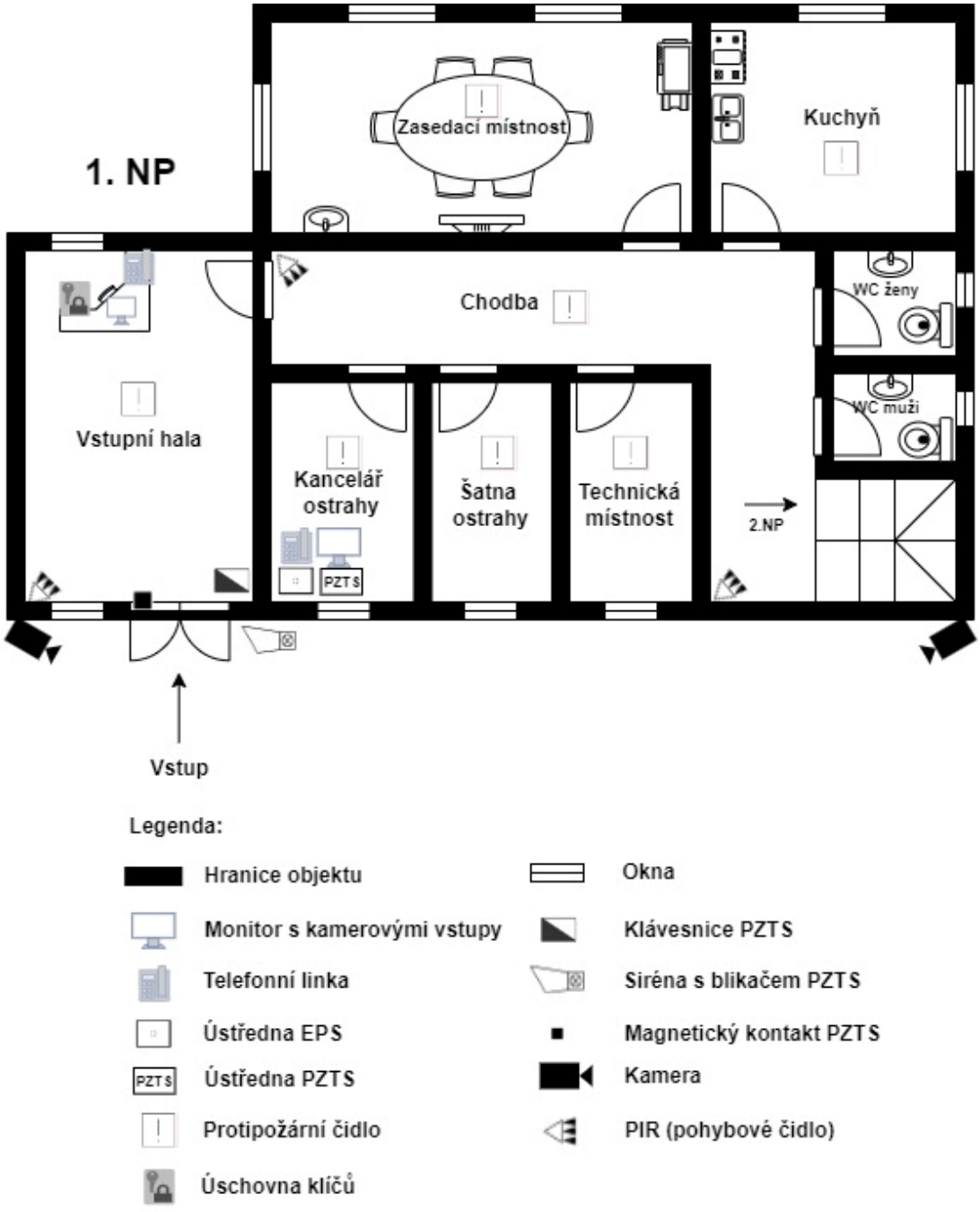
Jak již bylo zmíněno výše v textu, ředitel určuje zaměstnance, kteří mohou nakládat s utajovanými informacemi. Seznam těchto osob je uschován na příslušném oddělení v kanceláři budovy a jednu kopii vlastní i kancelář ostrahy. Pohybovat se v zabezpečené oblasti může jen osoba s oprávněním pohybu, tyto osoby zodpovídají za správné používaní technických prostředků a musí dodržovat pravidla zabezpečené oblasti. Zaměstnanec by měl postupovat následovně:

1) vždy před vstupem do místnosti zkontrolovat uzamčení dveří a až následně přikládat svojí ID kartu,
2) po vstoupení do místnosti s utajovanými informacemi zhodnotit celkový stav místnosti (například stav oken),
3) při odchodu z této místnosti musí zaměstnanec uzavřít okna, vypnout elektrická zařízení a uzamknout místnost, poté aktivuje zadáním kódu na klávesnici PTZS.

Technické prostředky

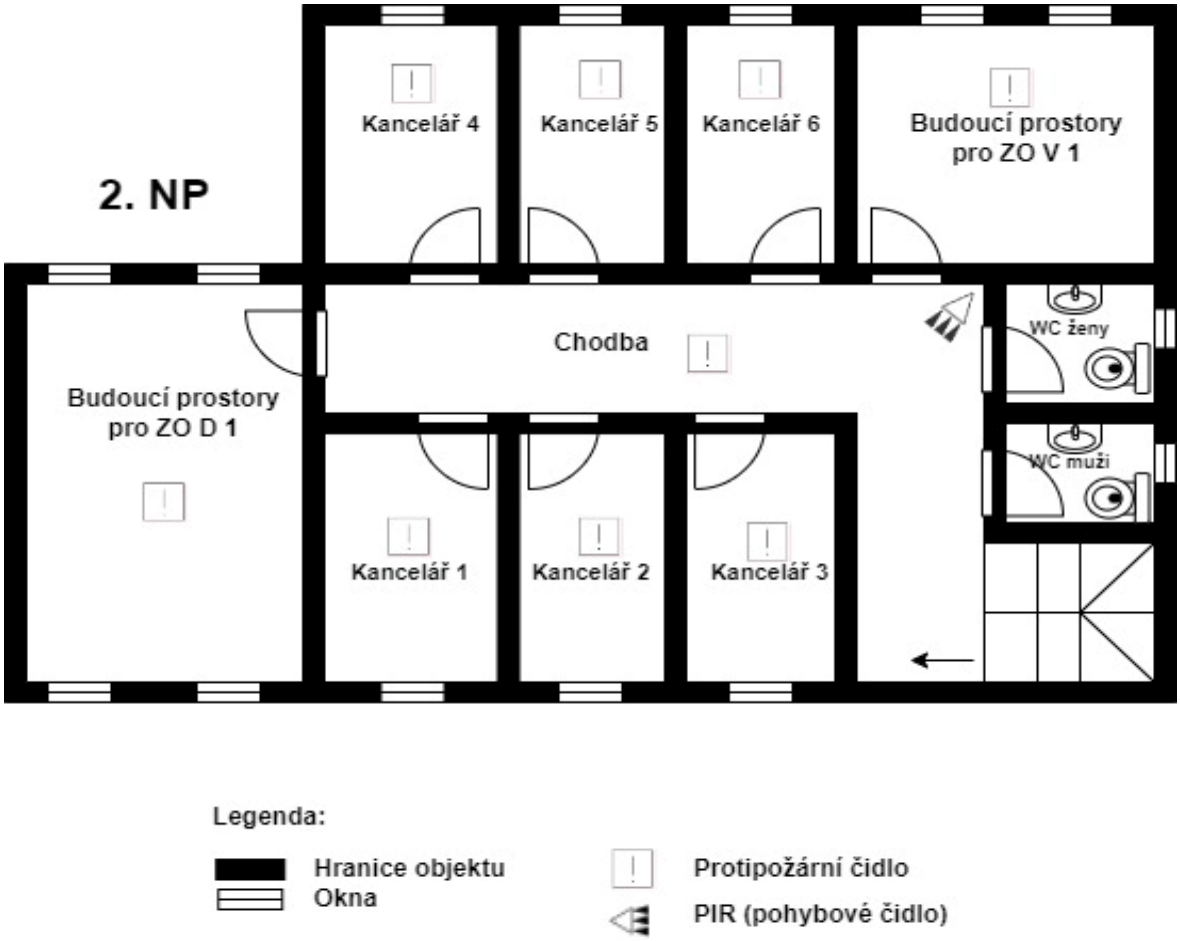
Zhodnocení předchozího technického stavu budovy pro budoucí analýzu FMEA. K zhodnocení technického stavu dopomáhá půdorys prvního a druhého nadzemního podlaží, které obsahují veškeré instalované technické prostředky. Půdorysy jsou umístěny pod tímto odstavcem.

Budova, než změnila režim fungování, byla osazena funkčním PZTS systémem doplněný elektronickou požární signalizací a částečným kamerovým systémem. Kamery byly osazeny pouze dvě s umístěním na rozích budovy a jejich ohnisko směřovalo na vstup budovy. Elektronický požární systém je aktuální a v budově se dále nerozšiřoval. Ústředna EPS je umístěna v kanceláři ostrahy. Čidla tohoto systému byla instalována v každé místnosti budovy. Poplachový zabezpečovací a tísňový systém byl instalován v předchozím stavu následovně. První nadzemní podlaží bylo osazeno PIR detektory s umístěním ve vstupní hale a na chodbě za vstupní halou a u hlavního schodiště do druhého nadzemního podlaží. Dále na hlavních dveřích budovy byl osazen magnetický kontakt snímání polohy dveří. Další magnety v budově nebyly osazeny. Hned za vstupními dveřmi po pravé straně byla instalována klávesnice systému, která má za funkci aktivaci a deaktivaci systému PZTS. Před budovu firma, která prováděla předešlou instalaci, osadila na fasádu pro případ cizího vniknutí akustickou sirénu s blikačem pro co největší upozornění na problém. V druhém patře byl osazen pouze jeden PIR detektor, a to v místech za schodištěm z prvního patra. Úplná absence byla v podání EKV systému, kdy princip odemykání a zamykání jednotlivých místností fungoval tak, že zaměstnanci budovy měli proti podpisu zapůjčovány klíče od dveří, kde vykonávali svou práci, příslušníkem ostrahy, který seděl ve vstupní hale.



Obrázek 9 – Půdorys 1.NP, původní stav

(Autor vlastní, vytvořeno v programu draw.io)



Obrázek 10 – Půdorys 2.NP, původní stav

(Autor vlastní, vytvořeno v programu draw.io)

9 ANALÝZA RIZIK

K použití analýzy FMEA potřebujeme sestavit tým odborníků, kteří vytvoří seznam možných vad a následků. V případě objektu X to bude odborník na aplikaci analýzy rizik a zástupci certifikovaných firem, kteří na základě objednávky od ředitele objektu zhodnotí společně stávající stav a navrhnou možná opatření ke zlepšení zabezpečení. Po provedeném brainstormingu se tyto návrhy pak za účasti všech přepíší do předem připravených protokolů, ve kterých se určí následek, výskyt a pravděpodobnost odhalení vady, ke každému kritériu se přiřadí číslo, které bude znázorňovat závažnost jednotlivé vady. Vynásobením všech vad, vznikne rizikové číslo, které nám určí, do jaké míry je riziko vážné. Aplikace analýzy FMEA se bude orientovat na fyzickou bezpečnost a původní stav zabezpečení objektu. Přehledové tabulky a samotné protokoly analýzy jsou zobrazeny pod tímto odstavcem.

Tabulka 2 – Kritéria významu vady

Číslo	Význam vady	Popis vady
1	Sotva postřehnutelný	Žádný důsledek
2-3	Nepatrný	Občasná, běžná, nezásadní porucha/vada
4-6	Středně závažný	Porucha vyvolá pozornost, ale není tak vážná
7-8	Velký	Výskyt závažné poruchy
9-10	Mimořádně závažný	Význam chyby mimořádně vysoký; ohrožení bezpečnosti systému a legislativní předpisy

(Vargová, Božek)

Tabulka 3 – Kritéria výskytu vady

Číslo	Výskyt vady	Popis
1	Nepravděpodobná	Chyba je skoro vyloučená
2-3	Nepatrná	Systém je pod kontrolou; ojedinělé vady
4-6	Malá	Systém je pod kontrolou; vady v malém rozsahu
7-8	Velká	Systém není pod kontrolou; vady se vyskytují často
9-10	Velmi vysoká	Chybě nelze zabránit

(Vargová, Božek)

Tabulka 4 – Pravděpodobnost odhalení vady

Číslo	Pravděpodobnost odhalení vady	Popis
1	Vysoká	Vysoké zabezpečení, které odhalí možnou vadu
2-5	Mírná	Metody zabezpečení můžou odhalit možnou vadu
6-8	Malá	Metody zabezpečení pravděpodobně odhalí možnou vadu
9	Velmi malá	Metody zabezpečení sotva odhalí možnou vadu
10	Nepravděpodobná	Metody zabezpečení systému nezjistí, anebo nemůžou zjistit možnou vadu

(Vargová, Božek)

Tabulka 5 – Rizikové číslo a jeho rozsah

Rizikové čísla (RN)	
Akceptovatelné riziko	RN ≤ 10
Významné riziko	10 <RN ≤ 100
Nepřijatelné riziko	RN> 100

(Vargová, Božek)

Tabulka 6 – Analýza FMEA (Poplachový zabezpečovací a tísňový systém)

Objekt: Budova X										**Číslo protokolu FMEA: 1**					
Odpovědná osoba: Tomáš Wencel										**Datum zpracování: 03/2023**					
ANALÝZA SOUČASNÉHO STAVU FYZICKÉ BEZPEČNOSTI – 1.NP, 2.NP										**BUDOUCÍ STAV FYZYCKÉ BEZPEČNOSTI**		**ANALÝZA STAVU PO PROVEDENÍ OPATŘENÍ**			
PRVEK	**MOŽNÁ CHYBA**	**MOŽNÉ NÁSLEDKY CHYBY**	**VÝZNAM**	**MOŽNÁ PŘÍČINA CHYBY**	**VÝSKYT**	**STAVAJÍCÍ OPATŘENÍ**	**STAVAJÍCÍ ŘÍZENÍ PROCESU**	**ODHALENÍ**	**RIZIKOVÉ ČÍSLO (RN)**	**NÁVRH OPATŘENÍ**	**ODPOVĚDNOST**	**VÝZNAM**	**VÝSKYT**	**ODHALENÍ**	**RIZIKOVÉ ČÍSLO (RN)**
POPLACHOVY ZABEZPEČOVACÍ A TÍSŇOVÝ SYSTÉM (PZTS)	Absence magnetických kontaktů oken	Vniknutí pachatele do budovy	7	Nedostatečný rozsah instalace PZTS systému	7	Žádné	Žádné	8	**441**	Doplnění mag. kontaktů certifikovanou firmou	Ředitel instituce	3	3	1	**9**
	Absence PIR čidel v nezab. místnostech	Nezachycený pohyb pachatele	8	Nedostatečný rozsah instalace PZTS systému	8	Žádné	Žádné	8	**512**	Doplnění PIR čidel certifikovanou firmou	Ředitel instituce	3	3	1	**9**
	Absence panic tlačítka	Pozdní přivolání pomoci	4	Nedostatečný rozsah instalace PZTS systému	4	Žádné	Žádné	5	**80**	Doplnění panic tlačítka certifikovanou firmou	Ředitel instituce	3	2	1	**6**
	Nefunkčnost PZTS systému	Nezabezpečení budovy	9	Výpadek elektrické energie / vadný záložní zdroj ústředny	9	žádné	Žádné	8	**512**	Beze změn/pravidelná kontrola zál.zdroje certifikovanou firmou	Ředitel instituce	4	2	1	**8**

Tabulka 7 – Analýza FMEA (Elektronická kontrola vstupů)

Objekt: Budova X									**Číslo protokolu FMEA: 2**					
Odpovědná osoba: Tomáš Wencel									**Datum zpracování: 03/2023**					
ANALÝZA SOUČASNÉHO STAVU FYZICKÉ BEZPEČNOSTI – 1.NP, 2.NP									**BUDOUCÍ STAV FYZYCKÉ BEZPEČNOSTI**		**ANALÝZA STAVU PO PROVEDENÍ OPATŘENÍ**			
PRVEK	**MOŽNÁ CHYBA**	**MOŽNÉ NÁSLEDKY CHYBY**	**VÝZNAM**	**MOŽNÁ PŘÍČINA CHYBY**	**VÝSKYT**	**STAVAJÍCÍ OPATŘENÍ**	**STAVAJÍCÍ ŘÍZENÍ PROCESU**	**ODHALENÍ**	**RIZIKOVÉ ČÍSLO (RN)**	**NÁVRH OPATŘENÍ**	**ODPOVĚDNOST**	**VÝZNAM**	**VÝSKYT**	**ODHALENÍ**	**RIZIKOVÉ ČÍSLO (RN)**
ELEKTRONICKÁ KONTROLA VSTUPŮ (EKV)	Absence celého systému EKV	Nekontrolovatelné vstupy do místností	7	Nedůsledná evidence zapůjčených klíčů	3	Režim úschovy klíčů	Vnitřní předpis	5	105	Oslovení certifikované firmy, realizace systému v celém objektu	Ředitel instituce	3	3	1	9

Tabulka 8 – Analýza FMEA (Elektronická požární signalizace)

Objekt: Budova X										**Číslo protokolu FMEA: 3**					
Odpovědná osoba: Tomáš Wencel										**Datum zpracování: 03/2023**					
ANALÝZA SOUČASNÉHO STAVU FYZICKÉ BEZPEČNOSTI – 1.NP, 2.NP										**BUDOUCÍ STAV FYZYCKÉ BEZPEČNOSTI**		**ANALÝZA STAVU PO PROVEDENÍ OPATŘENÍ**			
PRVEK	**MOŽNÁ CHYBA**	**MOŽNÉ NÁSLEDKY CHYBY**	**VÝZNAM**	**MOŽNÁ PŘÍČINA CHYBY**	**VÝSKYT**	**STAVAJÍCÍ OPATŘENÍ**	**STAVAJÍCÍ ŘÍZENÍ PROCESU**	**ODHALENÍ**	**RIZIKOVÉ ČÍSLO (RN)**	**NÁVRH OPATŘENÍ**	**ODPOVĚDNOST**	**VÝZNAM**	**VÝSKYT**	**ODHALENÍ**	**RIZIKOVÉ ČÍSLO (RN)**
ELEKTRONICKÁ POŽÁRNÍ SIGNALIZACE (EPS)	Výpadek celého systému	Nedetekování požáru	7	Výpadek elektřiny/nefunkční záložní zdroje ústředny	3	Roční kontroly certif. firmou	Předpis PBŘ	2	**42**	Nákup záložního zdroje objektu/beze změn	Ředitel instituce	4	2	1	**8**
	Vadné čidlo EPS	Nedetekování požáru	6	Výpadek ústředny/mechanické poškození	2	Roční kontroly certif. firmou	Předpis PBŘ	2	**24**	Beze změn	Certifikovaná firma	6	2	2	**24**
	Vadné tlačítko EPS	pozdní ohlášení požáru	4	Výpadek ústředny/mechanické poškození	2	Roční kontroly certif. firmou	Předpis PBŘ	2	**16**	Beze změn	Certifikovaná firma	4	2	2	**16**
	Vadná ústředna	Nedetekování požáru	7	Výpadek elektřiny/ vadná elektronika ústředny	2	Roční kontroly certif. firmou	Předpis PBŘ	2	**28**	Nákup záložního zdroje objektu/beze změn	Ředitel instituce/certifikovaná firma	4	2	2	**16**

Tabulka 9 – Analýza FMEA (Kamerový systém)

Objekt: Budova X											**Číslo protokolu FMEA: 4**			
Odpovědná osoba: Tomáš Wencel											**Datum zpracování: 03/2023**			
ANALÝZA SOUČASNÉHO STAVU FYZICKÉ BEZPEČNOSTI – 1.NP, 2.NP									**BUDOUCÍ STAV FYZYCKÉ BEZPEČNOSTI**		**ANALÝZA STAVU PO PROVEDENÍ OPATŘENÍ**			
PRVEK	**MOŽNÁ CHYBA**	**MOŽNÉ NÁSLEDKY CHYBY**	**VÝZNAM**	**MOŽNÁ PŘÍČINA CHYBY**	**VÝSKYT**	**STAVAJÍCÍ OPATŘENÍ**	**STAVAJÍCÍ ŘÍZENÍ PROCESU**	**ODHALENÍ**	**RIZIKOVÉ ČÍSLO (RN)**	**NÁVRH OPATŘENÍ**	**ODPOVĚDNOST**	**VÝZNAM**	**VÝSKYT**	**ODHALENÍ**	**RIZIKOVÉ ČÍSLO (RN)**
KAMEROVÝ SYSTÉM (CCTV)	Nefunkční kamerový systém	Nezachycení pachatele/neopr. vstup	7	Výpadek elektřiny/nefunkční komponenty	4	Žádné/ vizuální kontr.ostrahou	Vnitřní předpis	2	56	Nákup zál. zdroje objektu/ pravidelné kontroly cert.firmou	Ředitel objektu/ certifikovaná firma/ostraha	3	2	2	12
	Nefunkční venkovní kamera	Nezachycení pachatele/neopr. vstup	7	Výpadek elektřiny/přírodní vlivy	4	vizuální kontrola ostrahou	Vnitřní předpis	2	56	Pravidelné kontroly certifikovanou firmou	Certifikovaná firma/ostraha	3	2	1	6
	Absence kamer ve vnitřních prostorech	Nezachycení pachatele/neopr. vstup	8	Nedostatečný rozsah instalace CCTV/PZTS	8	Žádné	Žádné	9	576	Oslovení certifikované firmy, realizace systému vytipovaných míst	Ředitel objektu	3	2	2	12
	Absence kamer v budoucích zab.míst.	Nezachycení pachatele/neopr. vstup	8	Nedostatečný rozsah instalace CCTV/PZTS	8	Žádné	Žádné	9	576	Oslovení certifikované firmy, realizace systému vytipovaných míst	Ředitel objektu	3	2	2	12

Tabulka 10 – Analýza FMEA (Mechanické zábranné systémy)

Objekt: Budova X											**Číslo protokolu FMEA: 5**				
Odpovědná osoba: Tomáš Wencel											**Datum zpracování: 03/2023**				
ANALÝZA SOUČASNÉHO STAVU FYZICKÉ BEZPEČNOSTI – 1.NP, 2.NP										**BUDOUCÍ STAV FYZYCKÉ BEZPEČNOSTI**		**ANALÝZA STAVU PO PROVEDENÍ OPATŘENÍ**			
PRVEK	**MOŽNÁ CHYBA**	**MOŽNÉ NÁSLEDKY CHYBY**	**VÝZNAM**	**MOŽNÁ PŘÍČINA CHYBY**	**VÝSKYT**	**STAVAJÍCÍ OPATŘENÍ**	**STAVAJÍCÍ ŘÍZENÍ PROCESU**	**ODHALENÍ**	**RIZIKOVÉ ČÍSLO (RN)**	**NÁVRH OPATŘENÍ**	**ODPOVĚDNOST**	**VÝZNAM**	**VÝSKYT**	**ODHALENÍ**	**RIZIKOVÉ ČÍSLO (RN)**
MECHANICKÉ ZÁBRANNÉ SYSTÉMY (MZS)	Absence cert.okenních mříží	Vniknutí pachatele do budovy	7	Neoslovení certifikované firmy	8	Žádné	Žádné	9	**504**	Oslovení certifikované firmy, realizace systému vytipovaných míst	Ředitel objektu	3	3	1	**9**
	Absence cert.vstupních dveří	Nesplnění podmínek k utaj.informací	9	Neoslovení certifikované firmy	8	Žádné	Žádné	9	**648**	Oslovení certifikované firmy, realizace systému vytipovaných míst	Ředitel objektu	3	2	1	**6**
	Absence cert. vnitřních dveří	Nesplnění podmínek k utaj.informací	9	Neoslovení certifikované firmy	8	Žádné	Žádné	9	**648**	Oslovení certifikované firmy, realizace systému vytipovaných míst	Ředitel objektu	3	2	1	**6**
	Absence cert. elektronických zámků	Nefunkčnost budoucího EKV systému	9	Neoslovení certifikované firmy	8	Žádné	Žádné	9	**648**	Oslovení certifikované firmy, realizace systému vytipovaných míst	Ředitel objektu	3	3	1	**9**

10 SHRNUTÍ PROVEDENÉ ANALÝZY

Analýza fyzické bezpečnosti odhalila významné a nepřijatelné riziko. Z analýzy je zřejmé, že pro odstranění nedostatků bude potřeba součinnost specializovaných firem, ale i zdokonalení vnitřního předpisu. Jako možné chyby fyzické bezpečnosti byly určeny v protokolu FMEA 1 – PZTS chybějící magnetické kontakty, PIR detektory, panic tlačítko a nefunkčnost celého systému. U všech těchto zmíněných chyb bylo rizikové číslo stanoveno jako nepřijatelné riziko, což je pochopitelné, poněvadž absence čidel nebo funkčnost celého systému může mít dopad na zabezpečení celého objektu, proto certifikovaná firma, která se zapojila při vyhodnocování protokolu, bude nápomocna při odstraňování chyb tak, aby opětovná analýza po zavedení opatření snížila rizikové číslo na přijatelnou hodnotu.

Druhý protokol FMEA 2 – EKV hodnotil přítomnost a dopad elektronické kontroly vstupu, která v budově úplně chyběla. Tento protokol ukázal, že absence tohoto systému je považovaná za neakceptovatelné riziko i v případě stávajícího systému úschovny klíčů a jejich vydávání proti podpisu. Na základě tohoto protokolu se systém kontroly vstupu doplní, a bude se tak předcházet chybě lidského faktoru i s ohledem na budoucí práci objektu s utajovanými informacemi.

Třetí protokol FMEA 3 – EPS se zaměřil na již stávající a funkční systém elektronické požární signalizace, kde se spíš hledaly chyby ve funkčnosti systému a jeho koncových prvků, jako jsou tlačítka a detektory kouře. Tato analýza poukázala na to, že největší problém ve funkčnosti celého systému může být výpadek elektrického proudu nebo mechanické poškození, proto byl jako návrh opatření určen pořízení záložního zdroje pro celou budovu, i když v případě ústředny by měl být záložní zdroj součástí této ústředny. U tohoto zdroje se pak jedná spíše o zaměření se na pravidelné kontroly funkčnosti.

Čtvrtý protokol FMEA 4 – Kamerové systémy se s ohledem na absenci kamer uvnitř objektu zabýval tím, jak moc tato absence může ohrozit objekt a případné vniknutí do objektu, respektive nezachycení možného pachatele nebo pokus o neoprávněný vstup. Tyto chyby se ukázaly jako nepřijatelné, a proto se v případě fungování v režimu práce s utajovanými informacemi musí tyto kamery doplnit. Analýza se zaměřila i na výpadky elektrického proudu, kdy byl opět navržen záložní zdroj.

Poslední a v pořadí pátý protokol FMEA – Mechanické zábranné systémy měl za úkol určit rizikové číslo u plášťové a předmětové ochrany. Chybějící prvky poukázaly na úplnou nepřipravenost objektu a jeho mechanického zabezpečení. Proto se certifikovaná firma musí postarat zejména o koupi okenních mříží, vstupních a vnitřních dveří, které budou instalovány na budoucí místnosti zabezpečených místností pro práci v režimu vyhrazené a důvěrné, dále pak na osazení elektronických zámků, bez kterých by nefungovala elektronická kontrola vstupů. Tento protokol vyšel ze všech nejvážněji a byl zhodnocen jako nepřijatelné riziko ve všech bodech, je tedy v zájmu ředitele objektu o co nejrychlejší nápravu a eliminování rizika na přijatelnou hodnotu.

11 NÁVRH ZLEPŠENÍ ZABEZPEČOVACÍHO SYSTÉMU

Jelikož budova pracuje v novém režimu a nakládá s utajovanými informacemi, řídí se:

1) vyhláškou NBÚ č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů a,
2) normou ČSN EN 1627 (746001) s katalogovým kódem 514152 – dveře, okna, lehké obvodové pláště, mříže a okenice – odolnost proti vloupání – požadavky a klasifikace.

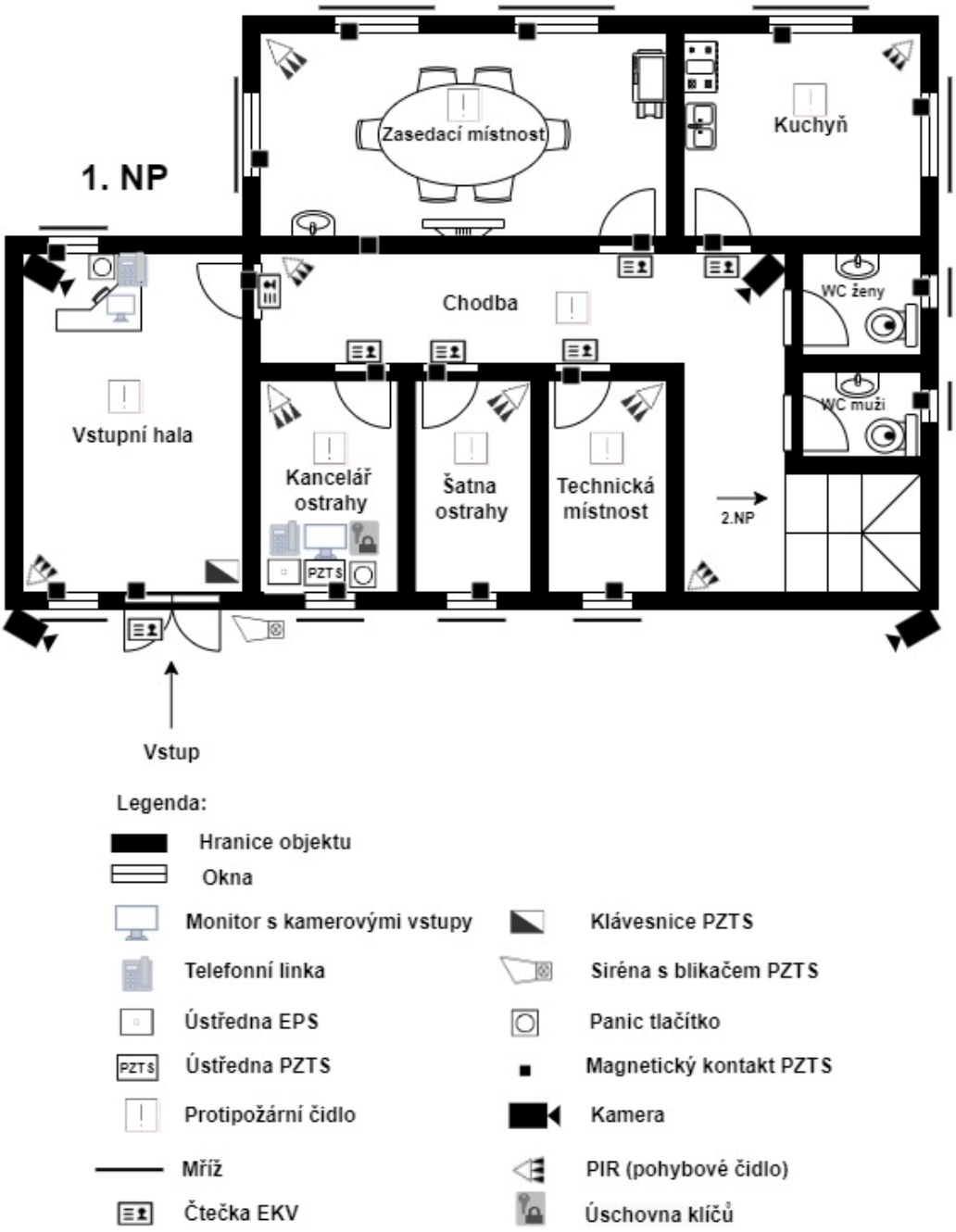
Proto, po změně režimu fungování budovy, byl rozšířen zejména systém PTZS o EKV systém, který se instaloval nově po celé budově. Tento systém představuje vylepšení stávajícího, sice funkčního ale zastaralého, půjčovaní jednotlivých klíčů. Proto se úschovna klíčů přemístila do kanceláře ostrahy, kdy nadále bude fungovat tento systém proti podpisu v případech například zapomenuté nebo ztracené ID karty. Identifikační karty jsou vydány uživateli na své jméno, mají v sobě uloženy přesně určená místa, kde uživatel této karty může vstoupit. Pro vstup do místnosti pak stačí pouze přiložit ID kartu k čtečce karet, následně čtečka změní barvu většinou na zelenou a přístup je povolen. V opačném případě, kdy jsou dveře zavřeny, svítí čtečka červeně. Pro vstup do zabezpečené zóny, tj. do místností, kde se nakládá s utajovanými informacemi, je nutné po přiložení ID karty a po vpuštění do této místnosti zadat na klávesnici PZTS přidělený deaktivační kód místnosti. Přístup a deaktivační kód mají pouze osoby s osvědčením pro nakládání s utajovanými informacemi. Jde tak o přehledný systém identifikující pohyb lidí po pracovišti a zamezuje neoprávněným osobám vstoupit tam, kde není jejich pracoviště.

Rozšíření stávajících prvků PZTS probíhalo tak, že se osadila všechna okna v prvním patře magnetickými kontakty ve vstupní hale, zasedací místnosti, kuchyni, na WC jak pánských, tak dámských, dále v kanceláři ostrahy, šatně ostrahy a technické místnosti. Tyto magnetické kontakty byly použity i na všechny dveře těchto místností. PIR detektory v tomto patře jsou nově osazeny ve všech místnostech kromě chodby a vstupní haly, kde už se tyto detektory nacházely v původní instalaci PZTS systému. Malé, ale nepatrné rozšíření systému PZTS bylo instalováno v podobě panic tlačítek, kdy tato tlačítka mají funkci přivolání pomoci, tzn. „tichá pomoc“. Instalace tlačítek proběhla ve vstupní hale ke stolu ostrahy a přímo do kanceláře ostrahy. Druhé patro bylo osazeno taktéž magnetickými kontakty na okna ve všech šesti kancelářích, na toaletách a v místnostech zabezpečené zóny, kde se nakládá

s utajovanými informacemi. Na všechny dveře, kromě toalet, byly rovněž osazeny magnetické kontakty. Do místností zabezpečených zón byly instalovány klávesnice pro deaktivaci PZTS systému místnosti. Ve druhém patře se rozšíření týkalo PIR detektorů. Tyto detektory se rozšiřovaly do každé místnosti, poněvadž v původní instalaci byl PIR detektor pouze u schodiště do druhého patra, což je pro naši budovu v tomto režimu nedostatečné.

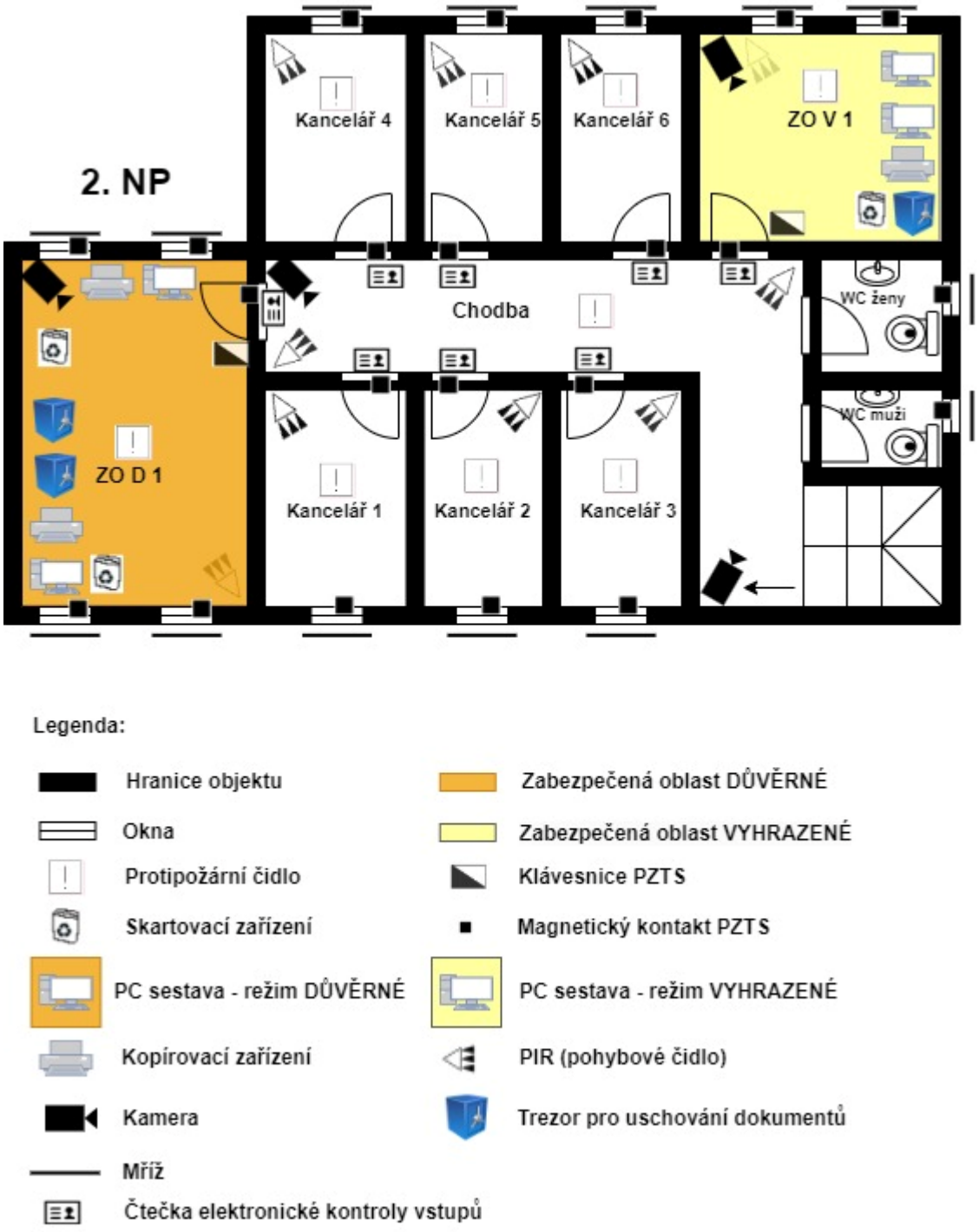
Mechanický zábranný systém byl podle certifikace rozšířen o nové vstupní dveře, o dveře do nově předělaných místností pro nakládání s utajovanými informacemi a celá budova byla doplněna předokenními mřížemi v obou patrech. Z důvodu nového rozšíření PTZS systému o EKV systém se na každé dveře, kromě WC, musely osadit certifikované elektronické zámky.

V neposlední řadě byl posilněn i kamerový systém, který se rozšířil zejména ve vnitřních prostorách budovy o jednu vnitřní kameru hned naproti vstupních dveří, dále o jednu kameru na chodbě umístěnou v rohu směrem ke schodišti do druhého patra a největší rozšíření se týkalo druhého nadzemního podlaží. V tomto patře byla kamera instalována hned u schodiště tak, aby zabírala i vstup do jedné z nově předělaných místností pro nakládání s utajovanými informacemi. Druhá kamera byla umístěna v rohu na konci celé chodby tohoto patra, opět tak, aby viděla na přicházející a odcházející zaměstnance z druhé místnosti pro nakládání s utajovanými informacemi. Do dvou místností se stupněm utajení Vyhrazené a Důvěrné byly osazeny kamery v rohu tak, aby snímaly pouze příchozí a odchozí.



Obrázek 11 – Půdorys 1.NP po návrhu zabezpečovacího systému

(Autor vlastní, vytvořeno v programu draw.io)



Obrázek 12 – Půdorys 2.NP po návrhu zabezpečovacího systému
(Autor vlastní, vytvořeno v programu draw.io)

Vedení tohoto objektu by mělo vždy při doplňování zabezpečovacích systémů nebo jakékoliv změně při práci s utajovanými informacemi postupovat dle platných zákonů, vyhlášek a norem určených pro certifikaci zabezpečovacích systémů, nebo práci s utajovanými informacemi uvedených v této bakalářské práci.

ZÁVĚR

Problematika utajovaných informací a zabezpečovacích systému byla hlavním cílem této bakalářské práce, přičemž se tato dvě témata přenesla na vybraný objekt, který má v budoucnu pracovat s utajovanými informacemi.

Teoretická část měla co nejlépe vystihnout již tak obsáhlá témata utajovaných informací a zabezpečovacích systémů. U obou témat byly popsány, pod jaké zákony a vyhlášky patří utajované informace a zabezpečovací systémy. Popsány byly taktéž druhy bezpečnosti, kterými se každý člověk nebo objekt musí řídit, aby mohl nakládat s utajovanými informacemi. Personální bezpečnost hovoří o podmínkách pro fyzické osoby, které pracují s utajovanými informacemi, administrativní bezpečnost pojednává o opatřeních, které plynou s nakládáním s utajovanou informací od jejího vzniku až po likvidaci této utajované informace. Fyzická bezpečnost má za úkol seznámit uživatele nebo objekt jak a čím zabránit neoprávněné osobě odcizit nebo zneužít utajovanou informaci. Jde především o aplikaci na daný objekt pomocí ostrahy, režimových opatření a technických prostředků.

Praktická část hovoří o samotném objektu X, kdy je popsána jeho poloha a umístění pomocí zkreslené mapky. Dále detailní popis vnitřních prostor před přechodem objektu na režim práce s utajovanými informacemi a po celkovém návrhu zlepšení zabezpečení pro práci s těmito informacemi. Pro vznik nákresu objektu byl využit program Draw.io.

Analýza FMEA, která byla vybrána pro účel této práce, měla za úkol navrhnout zlepšení bezpečnosti vybraného objektu, což se povedlo a důkazem jsou vytvořené protokoly analýzy FMEA. Protokoly nám skoro ve všech případech ukazují po návrhu opatření snížení rizikového čísla na akceptovatelné riziko, což je pro vybranou státní instituci vice než přijatelné. V případech, kdy se možná chyba a její snížení rizika neprojevilo tak markantně jako u ostatních chyb, se sice tak rizikové číslo nesnížilo, ale mezi akceptovatelným a významným rizikem takový rozdíl nebyl, což pro instituci může být opět přínosné. Pro tuto státní instituci je výhodné i získání praxe s analýzou FMEA, kdy tuto praxi s analýzou si v rámci vnitřního předpisu mohou vyhotovovat dle svého uvážení a aplikovat ji na cokoliv, co budou chtít zlepšovat, například v rámci personálních postupů nebo chodu objektu. Analýze však musí vždy předcházet brainstorming, ať už za pomoci nějakého odborníka, certifikované firmy, nebo v užším okruhu vedení instituce.

SEZNAM POUŽITÉ LITERATURY

Alarmtechnik.cz: Kamerové systémy, 2020. *Alarmtechnik.cz* [online]. Praha: Alarmtechnik Praha, spol. s r.o. [cit. 2023-03-08]. Dostupné z: https://www.alarmtechnik.cz/kamerove-systemy

BARTÁK, Jan, Jindrřich BEČVÁŘ a Miroslav BECHYNĚ, 1999. *Malá ilustrovaná encyklopedie: A-Ž*. Praha: Encyklopedický dům. ISBN ISBN 80-860-4412- 2.

BARTUŠEK, Jiří, 2015. Základní příručka elektronické požární signalizace. *APTjournal* [online]. [cit. 2023-03-08]. Dostupné z: https://www.atpjournal.sk/budovy/rubriky/prehladove-clanky/zakladni-prirucka-elektronicke-pozarni-signalizace.html?page_id=21297

BURDA, Karel, 2017. Základy elektronických zabezpečovacích systémů. Brno: Akademické nakladatelství CERM. ISBN 978-80-7204-967-7.

ČESKO, 2005. Vyhláška č. 528/2005 Sb. Vyhláška o fyzické bezpečnosti a certifikaci technických prostředků. Dostupné z: 528/2005 Sb. Vyhláška o fyzické bezpečnosti a certifikaci technických prostředků (zakonyprolidi.cz)

ČESKO, 2005. Zákon č. 412/2005 Sb.: Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti. *Zakonyprolidi.cz* [online]. [cit. 2023-03-09]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-412?citace=1

ČESKO, 2022. Vyhláška č. 275/2022 Sb.: Vyhláška o administrativní bezpečnosti a o registrech utajovaných informací. *Zakonyprolidi.cz* [online]. [cit. 2023-03-09]. Dostupné z: https://www.zakonyprolidi.cz/cs/2022-275/zneni-20230101?citace=1#p38_p38-1-1

ČESKO,2005. Nařízení vlády č. 522/2005 Sb. Nařízení vlády, kterým se stanoví seznam utajovaných informací. Dostupné z: 522/2005 Sb. Nařízení vlády, kterým se stanoví seznam utajovaných informací (zakonyprolidi.cz)

ČSN EN 50131-2-10 (334591): Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 10: Aplikace specifických požadavků na komunikátor ve střeženém prostoru, 2019. 2. Praha: Česká agentura pro standardizaci na základě ustanovení § 5 odst. 2 zákona č. 22/1997.

DEAN H. STAMATIS, 2019. *Risk Management Using Failure Mode and Effect Analysis (FMEA)*. ISBN 9780873899789. Dostupné také z: https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&an=2506716&scope=site

DELTA: 2D/3D DNR noise reduction [online], Poznań: DELTA-OPTI [cit. 2023-03-08]. Dostupné z: https://shopdelta.eu/2d3d-dnr-noise-reduction_l2_aid897.html

DVOŘÁK, Jan, Jiří CHROBÁK, 2018. *Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti: komentář*. Praha: Wolters Kluwer. Komentáře (Wolters Kluwer ČR). ISBN ISBN978-80-7598-016-8.

GRASSEOVÁ, Monika, Radek DUBEC a David ŘEHÁK, 2012. *Analýza podniku v rukou manažera: 33 nejpoužívanějších metod strategického řízení*. 2. vyd. Brno: BizBooks. ISBN ISBN978-80-265-0032-2.

HIKVISION, 2023. Přehled. *Www.hikvision.com:* [online]. Hangzhou Hikvision Digital Technology Co., Ltd. All Rights Reserved. [cit. 2023-03-08].

HLADÍK, Drahoslav, 2011. Elektronické zabezpečovací systémy a elektronická poţární signalizace. In: *Střední odborné učiliště Plzeň* [online]. Plzeň: SOUE Plzeň [cit. 2023-03-08]. Dostupné z: https://www.souepl.cz/wp-content/uploads/2020/09/elektronick%C3%A9-zabezpe%C4%8Dovac%C3%AD-syst%C3%A9my-a-elektronick%C3%A1-po%C5%BE%C3%A1rn%C3%AD-signalizace.pdf

HONEY, Gerard, 1999. *Electronic Security Systems Pocket Book*. GB: Newnes. ISBN 13: 9780750639910.

Kameryskladem.cz, Typy kamerových systémů, 2020. *Kameryskladem.cz* [online]. Frýdek-Místek: Kamery Skladem [cit. 2023-03-08]. Dostupné z: http://www.kameryskladem.cz/content/7-cctv-kamerove-systemy-typy-kamerovych-setu

KEGLEY, Ch. W. a E. R. WITTKOPF, 2006. *World Politics. Trends and Transformation*. Belmont: Thomson Learning. ISBN 0-534-60220-7.

KLOBOUČKOVÁ, Sylvie, 2015. *UTAJOVANÉ INFORMACE*. Praha. Dostupné také z: https://dspace.cuni.cz/bitstream/handle/20.500.11956/1120/150030355.pdf?sequence=1&isAllowed=y. RIGORÓZNÍ PRÁCE. Univerzita Karlova v Praze Právnická fakulta. Vedoucí práce JUDr. Jakub Handrlica, LL.M., Ph.D.

KOLOUCH, Jan, BAŠTA, Pavel 2019. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o. CZ.NIC. ISBN ISBN978-80-88168-31-7.

KŘEČEK, Stanislav, 2003. *Příručka zabezpečovací techniky*. Vyd. 2. [S.l.: s.n.]. ISBN 80-902-9382-4.

LUKÁŠ, Luděk, 2012. *Bezpečnostní technologie, systémy a management*. Zlín: Radim Bačuvčík - VeRBuM. ISBN 978-80-87500-19-4.

LUKÁŠ, Luděk, 2015. *Bezpečnostní technologie, systémy a management*. Vyd. 2. Zlín: Radim Bačuvčík - VeRBuM. ISBN 978-80-87500-67-5.

LUKÁŠ, Luděk, JAŠEK, Roman 2015. *Bezpečnostní technologie, systémy a management*. Zlín: Radim Bačuvčík - VeRBuM. ISBN 978-80-87500-67-5.

LUKÁŠ, Luděk,IVANKA, Ján 2014. *Bezpečnostní technologie, systémy a management*. Zlín: Radim Bačuvčík - VeRBuM. ISBN 978-80-87500-57-6.

MATIC, Luka, 2021. *Electronic Security and Espionage*. London: Elektor international media. ISBN 3895764655.

MICROSEGUR: WHAT IS WDR? WIDE DYNAMIC RANGE [online]. Madrid: Galleon Communication [cit. 2023-03-08]. Dostupné z: https://microsegur.com/en/what-is-wdr-wide-dynamic-range/

NBU. Informace. *Nbu.cz* [online]. [cit. 2023-03-08]. Dostupné z: https://www.nbu.cz/cs/ochrana-utajovanych-informaci/administrativni-bezpecnost-tvori-system-opatreni-pri-tvorbe-prijmu-evidenci-zpracovani-odesilani-preprave-prenaseni-ukladani-skartacnim-rizeni-archivaci-pripadne-jinem-nakladani-s-utajovanymi-informacemi/987-informace/

NBU. Obecně k personální bezpečnosti. *Nbu.cz* [online]. [cit. 2023-03-08]. Dostupné z: https://www.nbu.cz/cs/ochrana-utajovanych-informaci/personalni-bezpecnost-oznameni-pro-v-osvedceni-d-t-pt-certifikaty/1043-obecne-k-personalni-bezpecnosti/

POKORNÝ, Michal, 2019. Návrh zabezpečovacích a datových systémů v budově. In: ČVUT DSpace [online]. Praha: České vysoké učení technické [cit. 2021-03- 26]. Dostupné z: https://dspace.cvut.cz/handle/10467/82478

PROF. ING. BOŽEK CSC., František a Slavomíra ING. VARGOVÁ, PHD. Failure Mode and Effect Analysis Fehler Möglichkeits und Einfluss Analyse Analýza způsobů a důsledků poruch. In: *Moodle.utb.cz* [online]. Zlín [cit. 2023-03-26]. Dostupné z: https://moodle.utb.cz/pluginfile.php/769903/mod_resource/content/0/T%C3%A9ma%202b%20-%20Failure%20Mode%20and%20Effect%20Analysis%20-%20FMEA_Bozek.pdf

REDAKCE, 2021. Stupeň krytí (IP) udává ochranu telefonu před kapalinou a prachem. *Alza* [online]. [cit. 2023-03-08]. Dostupné z: https://www.alza.cz/stupen-kryti-ip

SHEEHAN, Michael, 2005. *International Security. An Analytical Survey*. London: London: Lynne Rienner Publishers. ISBN 978-1-58826-298-1.

ŠIMÍČEK, Jiří, 2015. Pyramida bezpečnosti. *Bezpečnostní poradenství JŠ* [online]. © 2015 Všechna práva vyhrazena. [cit. 2023-03-07]. Dostupné z: https://www.bp-js.cz/fyzicka-ochrana/

TINT: IR přísvit, *Kamerové systémy Tint* [online]. Frýdek-Místek: TINT [cit. 2023-03-08]. Dostupné z: https://www.kamerove-systemy-tint.cz/ir-prisvit/

TRADE FIDES. EKV. FIDES [online], 2019. [cit. 2023-03-07]. Dostupné z: https://www.fides.cz/technologicke-prostredky/ekv.html

TROCH. Kamerové systémy CCTV. *Trochsro.cz* [online]. [cit. 2023-03-08]. Dostupné z: http://trochsro.cz/slaboproud/kamerove-systemy-cctv/

VÁVRA, Dominik. Bezpečnostní prostředí v kontextu ochrany měkkých cílů. Zlín: Univerzita Tomáše Bati ve Zlíně, 2020, 72 s. Dostupné také z: Bezpečnostní prostředí v kontextu ochrany měkkých cílů (utb.cz). Univerzita Tomáše Bati ve Zlíně. Fakulta logistiky a krizového řízení, Ústav ochrany obyvatelstva. Vedoucí práce Rak, Jakub.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

PZTS	poplachový zabezpečovací a tísňový systém
MZS	mechanické zábranné systémy
EKV	elektronická kontrola vstupu
EPS	elektronická požární signalizace
HZS	hasičský záchranný sbor
DPPC	dohledové poplachové a přijímací centrum
CCTV	cloused circuit televison (uzavřený televizní okruh)
NBÚ	Národní bezpečnostní úřad
FMEA	Failure Mode and Effect Analysis (analýza možných vad a následků)

SEZNAM OBRÁZKŮ

SEZNAM TABULEK