Bezpečnostní management sídla justice

The Security Management of Seats of Justice

Bc. Martin Klásek

Diplomová práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Martin KLÁSEK**
Osobní číslo:	**A10423**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Bezpečnostní management sídla justice**

Zásady pro vypracování:

1. **Proveďte analýzu současného stavu zabezpečení.**
2. **Zpracujte zabezpečení budovy, vstup a únikových východů.**
3. **Navrhněte inovaci stávajích poplachových systémů.**
4. **Sociotechnický audit jednotlivých skupin justičních zaměstnanců.**
5. **Optimalizace systému zabezpečení.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **KŘEČEK, Stanislav. Příručka zabezpečovací techniky. Vyd. 2. S.l.: Cricetus, 2003, 351 s. ISBN 80-902-9382-4**
2. **FRIEDMAN, George. The intelligence edge: how to profit in the information age. 1st ed. New York: Crown, c1997, 276 s. ISBN 06-096-0075-3.**
3. **BRABEC, František. Bezpečnost pro firmu, úřad, občana. 1.vyd. Praha: Public History, 2001, 400 s. ISBN 80-864-4504-6.**
4. **LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management I. 1. vyd. Zlín: VeRBuM, 2011, 316 s. ISBN 978-808-7500-057**
5. **VYMĚTAL, Dominik. Informační systémy v podnicích: teorie a praxe projektování. 1. vyd. Praha: Grada, 2009, 142 s. ISBN 978-802-4730-462**
6. **ŠTĚDROŇ, Bohumír. Manažerské řízení a informační technologie. 1. vyd. Praha: Grada, 2007, 156 s. ISBN 978-802-4720-524**

Vedoucí diplomové práce: **JUDr. Vladislav Štefka**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **24. února 2012**

Termín odevzdání diplomové práce: **15. května 2012**

Ve Zlíně dne 24. února 2012

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práce se zabývá zabezpečením sídla justice. Jako jsou soudy a státní zastupitelství. V teoretické části práce se zabýváme požadavky na zabezpečení budovy stanovené předpisy. Provedení analýzy rizika a shrnutí technických prostředku nyní použitých v dané budově. Zaměření se na sociotechnický audit jako jednu z možností ohrožení. Praktická část obsahuje návrh optimalizace daného systému s poukázáním na současnou situaci, a možnosti jejich změn.

Klíčová slova:

Justice, I&HAS, CCTV, Analýza rizik, Únikový východ, Kamery, Ostraha

ABSTRACT

This thesis is concerned with securing the seat of justice. As courts and prosecution offices. In the theoretical part we have the security requirements set building regulations. Performing risk analysis and summary of the technical means now used in the building. The socio technical audits as possibility of danger. The practical part includes optimization of the system with reference to the current situation and possibilities for change.

Keywords:

Justice, I&HAS, CCTV, Analysis of risk, Emergency exit, Cameras, Guarding

Nejdříve bych na tomto místě velmi rád poděkoval vedoucímu diplomové práce panu JUDr. Vladislavu Štefkovi za trpělivost, inspiraci, podporu a jeho pomoc při vedení během tvorby a trpělivost při konzultacích ohledně této práce.

Dále své rodině, za jejich trpělivost a podporu během celého studia na této škole.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/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);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/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 diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Cílem této diplomové práce je zhodnocení systému zabezpečení a nalezení její optimalizace pro sídlo justice. Sídlem justice rozumíme všechny budovy a areály správních orgánu ministerstva spravedlnosti. Patří jsem státní zastupitelství a soudy. Soudy dělíme na Nejvyšší soud, Nejvyšší správní soudy, vrchní soudy, krajské soudy a okresní soudy. Považují se dle zákona 6/2002sb. za účetní jednotky. Státní zastupitelstva a soudy jsou součástí kritické infrastruktury státu a zajišťují právní moc. Samotné zabezpečení daných budov nebo areálů je důležité z hlediska zajištění fungování státu, správní agendy daného úřadu, nakládání s utajovanými skutečnostmi.

K nejlepšímu zhodnocení dané problematiky se zaměříme na objekt okresních soudů. Je to takový první stupeň ve výkonu soudní moci. I když by se mohlo zdát, že zaobírat se nejnižším stupněm i z bezpečnostního hlediska není podstatné, je okresní soud nedílnou součástí celého právního systému. Jak vyplývá z různých odvětví bezpečnostních systémů, platí i zde, že celý systém je tak bezpečný jak jeho nejslabší článek.

V úvodu samotné práce provedeme analýzu daného objektu z hlediska bezpečnostního systému a dalším ochranám. Předně se zaměříme na kontrolu elektronické zabezpečovacího systému, následně na kamerový systém v dané budově. Dále zjistíme zajištění budovy proti vzniku požáru a možnosti následného zmírnění účinku mimořádné události. Shrneme si možnosti sociotechnického auditu a jeho zaměření na danou problematiku. Vzhledem k tomu, že je to sice opomíjené téma, ale v poslední době čím dál diskutované i z hlediska zabezpečení určitých systémů. Jako je možný únik utajovaných informacích, nebo sdělení informací ke snadnějšímu přístupu do objektu. Například obeznámením neoprávněné osoby s použitým systémem.

V poslední řadě se zaměříme na vstupy a únikové východy v dané budově. Obě zaměření mají spojitost jak se zabezpečovacím systémem a tak elektrickým požárním systémem. V případě únikových východu budeme hodnotit jejich dostatečnost a využitelnost v případě vzniku mimořádné události, jako nutná evakuace osob.

I. TEORETICKÁ ČÁST

1 ANALÝZA SOUČASNÉHO STAVU ZABEZPEČENÍ

Na základě přijatých adekvátních bezpečnostních opatření je vlastní bezpečnostní ochrana objektu zabezpečována kombinací ochrany objektu a ochranou osob v objektu.

Ochranou objektu se rozumí souhrn opatření a činností směřujících k předcházení nebo zamezení zneužití, vyzrazení, znehodnocení, ztrátě nebo odcizení předmětu chráněného zájmu uložených nebo zpracovaných v objektu. Takové zabezpečení je možné provést fyzickou ostrahou objektu, kde je komplex úkolů plněný osobami pověřenými ostrahou objektu. Režimovými opatřeními, kterými se rozumí podmínky a pravidla pro vstup a výstup do objektu, včetně vjezdu vozidel a činnost v objektu prováděna. Systém evidence, označování a ukládání klíčů, zamykání a pečetění místností. Provádění pochůzek a kontrol osobami fyzické ostrahy. Porušení těchto předpisů lze posuzovat jako hrubé porušení pracovní kázně.

A v poslední řadě technickými prostředky objektu, které jsou:

- Mechanické zábranné prostředky, pro znemožnění nebo ztížení přístupu k předmětu chráněného zájmu. Například dveře, mříže, folie, bezpečnostní rámy a skla.
- Zařízení elektrické zabezpečovací signalizace, jako soubor elektronických a elektromechanických prvků ke zjištění a vyhodnocení neoprávněného vstupu
- Tísňové systémy, součást EZS – zejména tísňové hlásiče
- Speciální televizní systémy
- Vstupní systémy elektrické pro zabezpečení vstupu a prokázání oprávnění a totožnosti osob.
- Zařízení elektronické požární signalizace je soubor prvků pro včasnou signalizaci vzniku požáru
- Detektory látek nebo zařízení pro vyhledávání kovu, výbušnin a polovodičů
- Zařízení proti pasivnímu a aktivnímu odposlechu s míst vně budovy
- Zařízení na ničení fyzických nosičů informací.

Ochranou osob se rozumí činnosti směřující k ochraně života a zdraví osob v objektu. Zejména v případě z vzniku mimořádných událostí a jejich řešení dle havarijních plánů.

Materiální zabezpečení, evakuace a ukrytí, vyrozumění a varování, činnost po oznámení umístění nástražného výbušného systému a případném výbuchu.

Mimořádnou událostí se rozumí škodlivé působení sil a jevů vyvolaných činností člověka, přírodními vlivy a havárií ohrožujících život, zdraví a majetek.

Podezřelým předmětem je takový předmět u něhož umístění, účel, původ, vnější forma, majitel nebo jiné okolnosti jeho výskytu nejsou známy nebo jsou podezřelé. Mohl by být nástražným systémem nebo nástražným výbušným systémem spadající. Patří jsem i poštovní zásilky vykazující znaky podezřelosti.

Nástražný výbušný systém je takový systém, který je tvořený výbušným předmětem, výbušnou látkou nebo pyrotechnickým prostředkem s funkčními prvky iniciace. Takový systém je schopný vyvolat za určitých předem stanovených podmínek výbuchový účinek nebo ložisko požáru. Bývá zpravidla ukryt v obale, nebo má takovou vnější formu aby utajil svůj pravý účel. Problém nastává v okamžiku kdy vzhled takového systému zejména u improvizovaných výbušných předmětů může mít různou velikost, tvar nebo složitost a nemusí na něj obecná definice platit.Může být například implantován jako běžná součást vybavení objektu. Ne vždy je na první pohled zřejmé, že se jedná o nástražný výbušný systém.[14]

V případě justičních sídel se zaměříme na výše uvedené oblasti. Pro oblast fyzické ostrahy je zřízena Justiční stráž zákonem 555/2002 sb. O Vězeňské službě a justiční stráži České republiky.

Justiční stráž dle § 2, odstavce 1f) *zajišťuje pořádek a bezpečnost v budovách soudů, státních zastupitelství a ministerstva a v jiných místech jejich činnosti a v rozsahu stanoveném tímto zákonem zajišťuje pořádek a bezpečnost při výkonu pravomoci soudů a státních zastupitelství*,

Práce justiční stráže je tedy z určitého pohledu shodná s prací fyzické ostrahy objektu, která má následující funkce:

- Kontrola přístupu, kdy zajišťujeme jednotlivé vstupy do objektu s cílem zamezit neoprávněnému přístupu.
- Vykonávání tzv. hlídek, kdy dochází ke kontrole prostoru objektu v daných časových intervalech.

- Doprovod a kontrola osob nebo materiálu tak aby se pohybovali od vstupu k cíli bez jakéhokoliv vychýlení z trasy.
- Prohlídka, jako prevence možných rizik a narušení bezpečnosti.
- Další úkoly jako jsou spolupráce při vyšetřování krádeží nebo škod, provádění fyzického průzkumu zabezpečení a ohodnocení zranitelnosti objektu, kontakty se složkami IZS, a další.

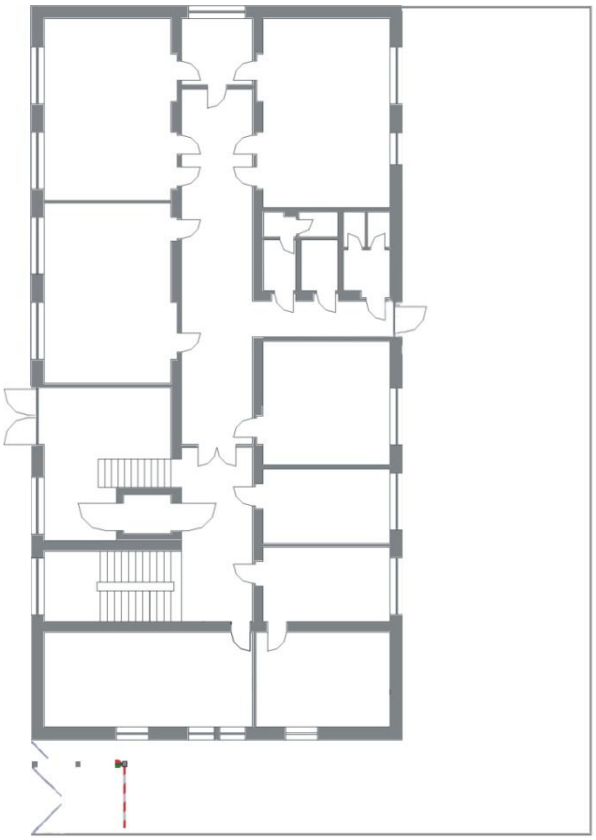
Strukturu justiční stráže tvoří zpravidla vedoucí pracovník, velitel, obvykle osoba s nejvyšší hodností. Jeho úkolem zajištění funkčnosti celého útvaru a stanovení úkolu jednotlivým členům. Komunikace s vedením daného soudu(předseda), bezpečnostním technikem a generálním ředitelstvím nebo vězeňskou službu pod kterou spadá.

1.1 Popis objektu

Soudní budova nebo spíš areál, kterým se zaobíráme, se nachází v centru města. Obklopen z jedné strany bytovou zástavbou a z druhé průmyslovým areálem. Budova byla postavena někdy v 70. letech minulého století jako funkcionalistický dům. Před deseti lety prošla nákladnou rekonstrukcí a následně pak modernizací bezpečnostních systémů. Půdorys budovy je tvořen klasickým obdélníkovým tvarem. A skládá se ze tří nadzemních a jednoho podzemního podlaží. Nachází se zde kanceláře, jednací místnosti, technické zázemí budovy a bezpečnostní místnost na dokumenty, spisy a další materiál s označením důvěrné. Ale tou se budeme zaobírat samostatně níže. Jednotlivá podlaží spojují dva výtahy a jedno schodiště, které je označované i jako jediná úniková cesta. Nedílnou součástí celého objektu je i tzv. venkovní prostor. Jedná se o prostor v zadní části budovy primárně určený pro parkování vozidel zaměstnanců a správy daného úřadu. Příjezdová cesta z přední části budovy je chráněna bezpečnostní závorou s dálkovým nebo klíčovým ovládáním během provozu, následně po skončení provozní doby je uzavřena uzamykatelnou bránou. Prostor závory je monitorován kamerou s černobílým zobrazením, pro lepší viditelnost v noci.

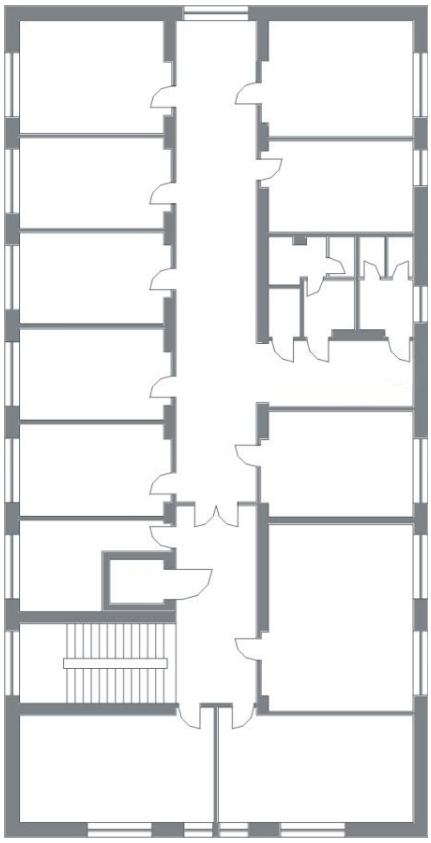
V prvním nadzemním podlaží se nachází jednak hlavní vstup do budovy, vybaven bezpečnostním rámem pro odhalení zbraní a jiných nebezpečných předmětů. Hlídaný

fyzickou ostrahou budovy, obvykle jedním členem justiční stráže, který zároveň obsluhuje i kamerový systém budovy. Následně vstoupíme do dlouhé chodby střežené jednou kamerou s detektorem pohybu a dvěma PIR detektory. S chodby máme vstup na schodiště nebo do výtahu vedoucích do dalších poschodí. Nebo do jednacích místností, kanceláře a pokladny s podatelnou. Každá místnost je vybavena minimálně PIR detektorem. V případě zasedacích místností jsou to i kamery, které dohlíží na bezpečnost při jednáních, ovšem je i možnost je na žádost soudce nebo státního zástupce, který jednání vede vypnout. Okna v prvním nadzemním podlaží jsou vybavena detektory pro případ jejich rozbití a magnetickými kontakty při otevření. Magnetické detektory jsou i na všech dveřích v celé budově. V tomto podlaží se nachází ještě vchod na parkovací plochu za budovou.



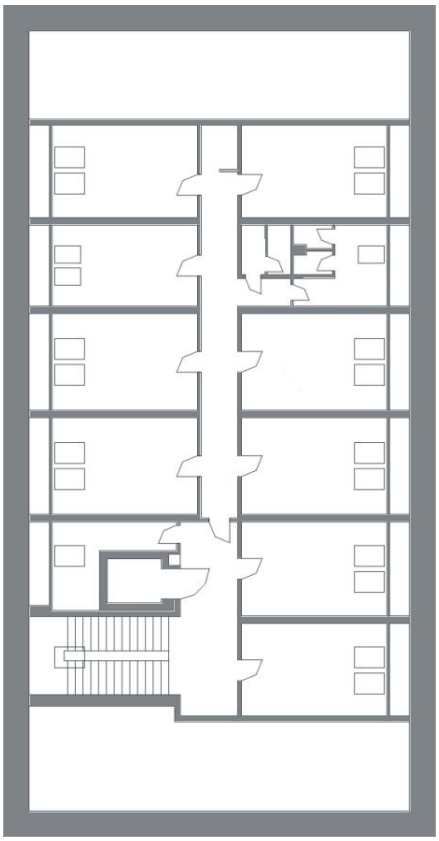
Obr. 1: 1. Nadzemní podlaží, zdroj: vlastní

Do druhého nadzemního podlaží se můžeme dostat buď výtahem, který ovšem v případě požáru není funkční, tedy není jej možné použít pro evakuaci osob. Nebo po standartním proskleném schodišti vybaveném otřesovými detektory pro případ rozbití skla a PIR čidly. Nevýhodou schodiště je pro propojení detektorů do jedné smyčky na celém schodišti, takže v případě poplachu nevíte, ve které části schodiště k narušení došlo. Po vstupu na 2. nadzemní podlaží se nacházíte na spíše na první dojem na menší chodbě se vstupem do jednacích místností a možností vstupu do kancelářských prostor oddělených prosklenou přepážkou. Vybavení místností je z hlediska zabezpečení stejné jako v prvním podlaží. Jistým bezpečnostním prvkem jsou i nouzová tlačítka v jednacích místnostech o kterých ví jen určené osoby, obvykle na místě pro soudce nebo osoby vedoucí jednání, kterým je možné v případě potřeby přivolat příslušníka justiční stráže. Ovšem občas docela nešikovně umístěné a proto dochází k jejich spuštění bezdůvodně.



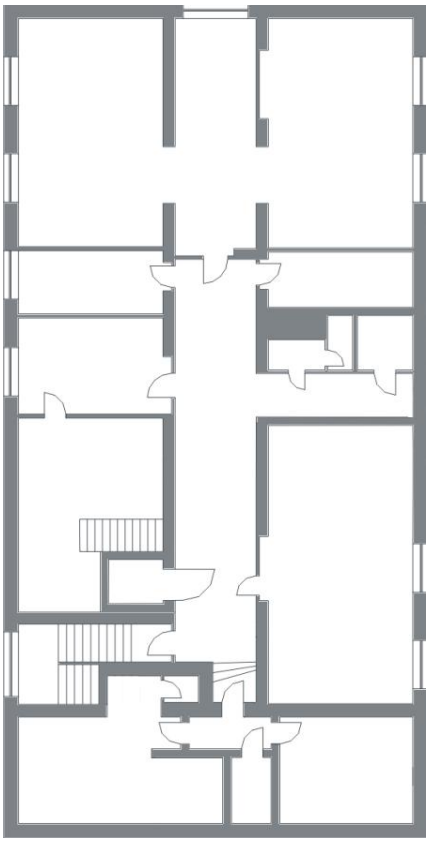
Obr. 2: 2. Nadzemní podlaží, zdroj: vlastní

Pokračujeme po schodišti dále až do posledního patra, kde se nachází už jen prostory pro správu a chod budovy. Místnosti pro uložení písemností, servery pro počítačovou síť a další prostory. Vše je zde pod dohledem kamer a PIR detektorů. Když to shrneme celá budova je pod neustálým dohledem kamer, ovšem bez možnosti nočního vidění, tedy kolikrát stačí na některých místech zhasnout světla, týká se to hlavně chodeb.



Obr. 3: 3. Nadzemní podlaží, zdroj: vlastní

Nyní se vydáme opačným směrem, tedy dolů. Budova má jedno podzemní podlaží, které je opět přístupné výtahem nebo po schodech, ovšem už jen s klíčem opravňujícím jeho majitele ke vstupu do daných prostor. Jsou zde na první pohled jen sklady, ale není tomu úplně tak. Je zde technické zázemí pro zabezpečovací techniku, tedy místnost se záznamovými zařízeními pro kamery, ústřednou EZS spojující jejich jednotlivé prvky a další systémy. Včetně připojení na pult centrální ochrany Policie České republiky. Jsou zde i dvě plně vybavené cely pro případ ubytování osoby čekající na vynesení rozsudku. Plně pod dohledem kamer s nouzovým tlačítkem na přivolání ostrahy. A dále běžné skladovací prostory a speciální místnost. Tato místnost je určená pro ukládání dokumentů a věcí s označením důvěrné, je vybavena kromě bezpečnostních prvků, které se používají v celé budově, také bezpečnostními dveřmi připomínající spíše trezor u nichž je další nouzové tlačítko a také tlačítko pro případ požáru. Tato místnost je jediná v celé budově, která je vybavena detektory kouře s automatickým hasícím systémem i s možností manuálního spuštění.



Obr. 4: 1. Podzemní podlaží, zdroj: vlastní

1.2 Analýza rizik

Na základě zjištěných skutečností sestavíme tabulku s bodovým hodnocením, abychom zjistili míru rizika a stanovili kategorii spadající do oblasti zabezpečeného objektu.

BEZPEČNOSTNÍ OPATŘENÍ	TYP	BODOVÉ OHODNOCENÍ
Úschovné objekty	□ T. 4 – 4 body □ T. 3 – 3 body □ T. 2 – 2 body □ T. 1 – 1 bod	SS 1 = 3
Zámky úschovných objektů	□ T. 4 – 4 body □ T. 3 – 3 body □ T. 2 – 2 body □ T. 1 – 1 bod	SS 2 = 2
Úschovný objekt včetně uzamykatelného systému	□ T. 1A – 1 bod □ T. 1B – 2 body □ T. 1C – 3 body □ T. 1T– 1 bod □ T.T– neuvedeno	S1 = 6
Celkové hodnocení úschovného objektu a jeho zámku	S1 = SS1 x SS2	S1 = 6
Zabezpečené oblasti	□ T. 4 – 4 body □ T. 3 – 3 body □ T. 2 – 2 body □ T. 1 – 1 bod	SS3 = 2
Uzamykatelné systémy zabezpečené oblasti	□ T. 4 – 4 body	

	□ T. 3 – 3 body □ T. 2 – 2 body □ T. 1 – 1 bod	SS4 = 2
Celkové hodnocení zabezpečené oblasti a jejího uzamykacího systému	S2 = SS3 x SS4	S2 = 4
Objekt	□ T. 4 – 5 bodů □ T. 3 – 3 body □ T. 2 – 2 body □ T. 1 – 1 bod	S3 = 0
Kontrola vstupu	□ T. 4 – 4 body □ T. 3 – 3 body □ T. 2 – 2 body □ T. 1 – 1 bod	SS6 = 1
Režim návštěv v objektu Návštěvy s doprovodem Návštěvy bez doprovodu¨ Návštěvy bez kontroly	□ ad a) – 3 body □ ad b) – 1 bod □ ad c) – 0 bod	SS7 = 0
Celkové hodnocení kontroly vstupu	S4 = SS6 + SS7	S4 = 1
Ostraha	□ T. 5 – 5 bodů □ T. 4 – 4 body □ T. 3 – 3 body □ T. 2 – 2 body □ T. 1 – 1 bod	SS8 = 1
Zařízení elektrické zabezpečovací signalizace	□ T. 4 – 4 body □ T. 3 – 3 body □ T. 2 – 2 body	SS91 = 3

	□ T. 1 – 1 bod	
Instalace zařízení elektrické zabezpečovací signalizace	□ T. 4 – 4 body □ T. 3 – 3 body □ T. 2 – 2 body □ T. 1 – 1 bod	SS92 = 3
Mezivýsledek (SS9)	SS9 = (SS91+SS92)/2 x SS92/OBL	SS9 = 4
Celkové hodnocení ostrahy a systému EZS	S5 = SS8 + SS9	S5 = 5
Fyzické bariéry	□ T. 7 – 12 bodů □ T. 6 – 9 bodů □ T. 5 – 7 bodů □ T. 4 – 4 body □ T. 3 – 3 body □ T. 2 – 2 body □ T. 1 – 1 bod	SS10 = 0
Kontrola vstupu v přístupových bodech fyzické bariéry a) Prohlídky jsou prováděny b) Kontrola není realizována	□ ad a) – 1 bod □ ad b) – 0 bodů	SS11 = 0
Namátkové vstupní a výstupní prohlídky a) Prohlídky jsou prováděny b) Prohlídky nejsou prováděny	□ ad a) – 1 bod □ ad b) – 0 bodů	SS12 = 0
Perimetrický detekční systém PDS	2 body	SS13 = 0
Bezpečnostní osvětlení perimetru	2 body	SS14 = 0
Speciální televizní systém perimetru	2 body	SS15 = 0

Celkové hodnocení ochrany perimetru	S6 = (SS10 x SS11) + SS12 + SS13 + SS14 + SS15	S6 = 0

Tabulka 1: Bezpečnostní opatření

Hodnoty proměnných S1 a S6 získané vyplněním shora uvedené tabulky, je nutné porovnat s tabulkou bodových hodnot nejnižší míry zabezpečení ZO. Na základě tohoto porovnání stanovit, zda jsou opatření fyzické bezpečnosti pro danou míru rizika a kategorii ZO dostatečná.

ZABEZPEČENÁ OBLAST KATEGORIE Důvěrné	Míra rizika		
	malá	střední	velká
Povinné: (S1) + (S2) + (S3) – požadovaná	6	8	9
Výsledná hodnota: vypočtená		10	
Povinné (S4) + (S5) – požadovaná	2	3	3
Výsledná hodnota: vypočtená		6	
Nepovinné: (S6)	3	3	4
Výsledná hodnota: vypočtená		0	
Celkový výsledek (požadovaná hodnota)	11	14	16
Celková výsledná hodnota		16	

Tabulka 2: Kategorie zabezpečené oblasti

Výpočet hodnoty NBU (S1 + S2 + S3) + (S4 + S5) + S6 = (6 + 4 + 0) + (1 + 5) + 0 = 10 + 6 + 0 = 16 (požadovaná hodnota dle NBÚ = 14)Pouze jedna z hodnot (S1), (S2) nebo (S3) může být rovna 0. Stanovený objekt, zabezpečenou oblast může využívat k činnosti související s ochranou UI pouze jeden orgán státu, právnická nebo podnikající fyzická osoba Použití uvedených bezpečnostních opatření vyhovuje požadavkům vyhlášky NBÚ č.

528/2005 Sb., o objektové bezpečnosti, a Bezpečnostních standardů NBÚ pro zabezpečenou oblast kategorie „DŮVĚRNÉ“.

Název komponentu, prvku	**Bodové ohodnocení**	**Číslo certifikátu NBÚ**	**Platnost certifikátu NBÚ**
Mechanické zábranné prostředky			
Mobilní skříňový trezor, IVETA 5 M	SS1 = 6	T0045/2011	24.3.2011
Bezpečnostní dveře NEXT typ SD 101	S2 = 6	T0090/2004	1.9.2007
Elektrická zabezpečovací signalizace			
Ústředna EZS ATS 4000	SS91 = 3	T1185/2004	6.10.2007
Duální čidlo DISCOVERY-DUO AM	SS91 = 3	T1019/2006	29.1.2009
Čidlo otevření MK 440	SS91 = 3	T1158/2004	20.8.2007
Tísňové tlačítko ART 476	SS91 = 2	T1083/2010	8.5.2010
Skartovací stroj HSM 108.2	Bez bod. ohodnocení		

Tabulka 3: Certifikáty NBU technických prostředků

1.3 Technologie

1.3.1 EZS/I&HAS

Zabezpečovacím prvkem EZS je ústředna ATS-4000 společnosti ARITECH. Zařízení má certifikaci NBU pro oblast Tajné, v modifikaci až přísně tajné. Daná ústředna zvládne až 16 ovládacích panelů, z čehož plyne i možnost rozdělení oblastí na 16 zón. Integrování přístupového systému je samozřejmosti a je součást zapínání a vypínání systému EZS. Pomocí expandérů je možné mít až 256vstupů a 255výstupů z jednotky včetně připojeni k siréně. Samotná ústředna má v sobě dva nezávislé deníky pro EZS a přístupový systém. Každý z nich má kapacitu až 1.000 záznamů. Pro připojení k PCO je zde telefonní

komunikátor, ale zároveň i možnost připojit další moduly. Například počítač s tiskárnou, ISDN a GSM modul a dále.

Obr. 5: Ústředna ATS-4000

zdroj:http://www.utcfssecurityproductspages.eu/SK/products_single.php?product=ATS4000

1.3.1.1 DISCOVERY DUO-AM

Jedná se o duální detektor pohybu odolný vůči falešným poplachů a antimaskingu. Pro vyšší spolehlivost detekce pohybu využívá cylindrickou čočku. Součástí je i technologie TRUE MOTION RECOGNITION pro opravdovou detekci pohybu lidského těla od jiných změn. Kloubí v sobě technologii PIR a MW, kdy dosah PIR je 12m a dosah MW je od 3 do 12m na frekvenci 2,45GHz. Schopnost pracovat v prostředí s teplotami od -10 do + 50°C.

Obr. 6: Discovery DUO-AM, zdroj: http://www.sicurit.cz

1.3.2 CCTV

Jedny z nejlepších a nejpoužívanějších kamerových systémů jsou zařízení společnosti Interlogix patřící do skupiny společností GE. Nově se bezpečnostní produkty skupiny GE staly součástí UTC Fire & Security family.

1.3.2.1 StoreSafe pro

StoreSafe je video multiplexer schopná nahrávat z více kamer na vestavěný pevný disk s možností současného přehrávání. Na rozdíl od zastaralých pomaloběžných videorekordérů nahrává StoreSafe obraz s vysokým rozlišením. Digitální nahrávka dosahuje vysoké kvality oproti běžnému videorekordéru a odpadají potíže při používání klasických videorekordérů. V závislosti na nastavení dokáže StoreSafe uchovávat barevné snímky od několika hodin až po více než tři roky.

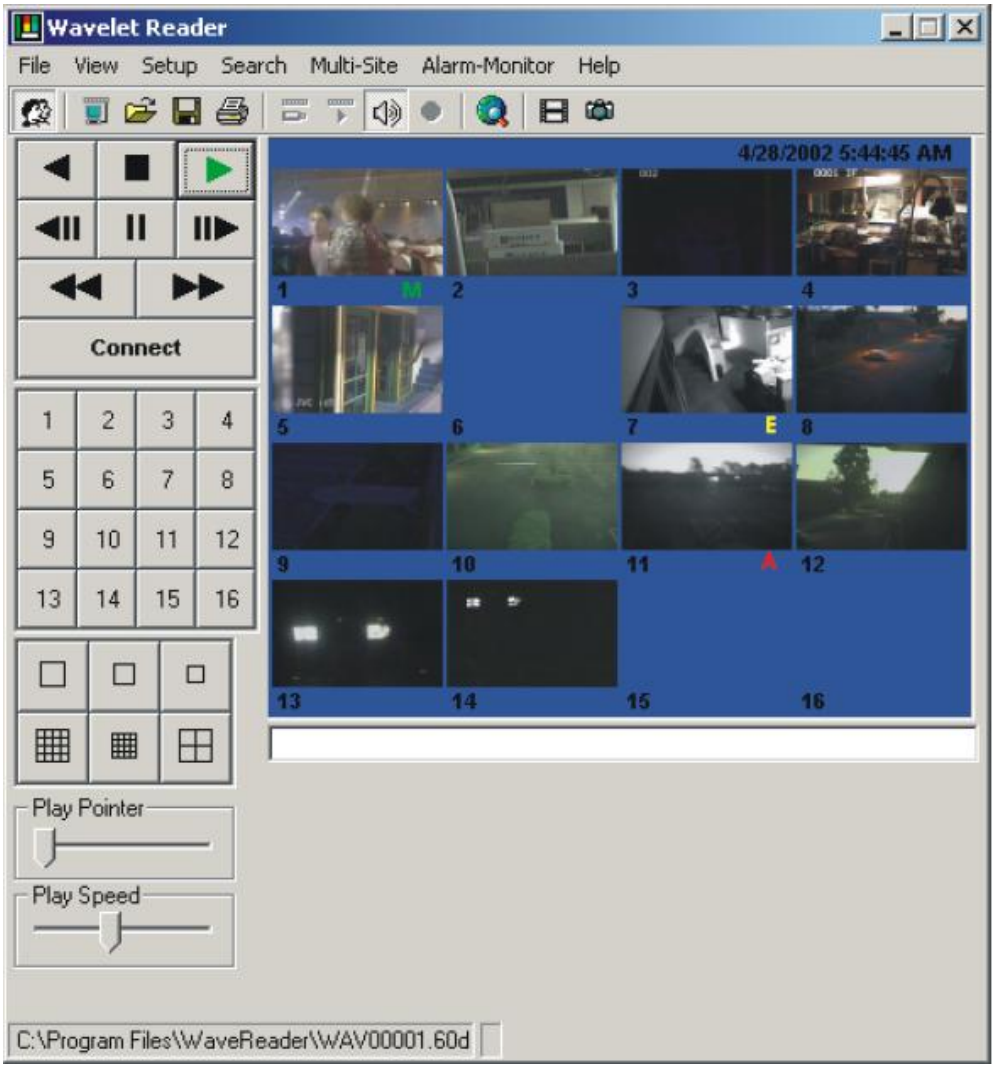
Programovatelné vyhledávání urychluje samotnou práci s daty pří jejím zpracování. Nahrané snímky nebo události vyhledá přístroj podle poplachu, času, datumu, výpadku signálu nebo čísla kamery. Pro zjednodušení ovládání je přístroj vybaven praktickými tlačítky pro jednoduché a rychlé ovládání tisku a archivace. Mezi jeho vlastnosti patří:

- Multiplexer s vestavěným digitálním nahráváním
- Přehrávání a živé prohlížení ve více oknech
- Nahrávání až 16 kamer rychlostí 25pps
- Dálkové programování a řízení
- Sledování živého či nahraného obrazu na dálku pomocí SW WaweReader
- Zobrazení na dvou monitorech
- Detekce pohybu v obraze (vloupání a aktivita)
- Zpracování poplachu se záznamem
- Nepřetržité nahrávání se simultánní archivací
- Synchronizace se síťovým serverem
- Tisk obrázku
- Dynamické adresování IP (DHCP)
- Upozornění na poplach

Obr. 7: StoreSafe Pro, zdroj: User Manuál StoreSafe Pro: Ge Security 2004

1.3.2.2 WaweReader

Jedná se o program umožňující sledování a přehrávání videa z různých zařízení, jako jsou digitální videorekordéry, rekordéry s multiplexem, digitální jednokanálové rekordéry nebo digitální záznamová zařízení. Pro svou komunikaci využívá sítě Ethernet nebo komunikačního modemu daných zařízení. Umí komunikovat s různými datovými nosiči, včetně pevného disku.Umožňuje sledování živého videa nebo záznamu. Grafickou analýzu zaznamenaných dat a vyhledávání dle data a času. Ovládání otočných kamer a tisk a úpravu snímku jak ze záznamu videa tak v reálném čase. Dobrou vlastnosti je režim Multi-site, který umožňuje zobrazení videa z více jednotek najednou. A možnost přepínání mezi Live režimem a režimem Playback.



Obr. 8: Program WaveReader zdroj: WaveReader User Manual:GE Security

1.3.2.3 KTD-405 klávesnice

Klávesnice KTD-405U zabezpečí ovládání multiplexerů a systémů Digiplex® z jednoho místa. Komunikační porty RS422/RS485 umožňují KTD-405U ovládat multiplexery DTX, DTXA, CyberDome a CyberScout kamery, přepínat kamery a monitory a iniciovat trasy kamer. Programovat je z klávesnice možno multiplexery, CyberDome, CyberScout, maticové přepínače a poplachová rozhraní.

Tříosý ovladač na vyjímečně precizní řízení natáčení a naklánění v aplikacích s otočnými kamerami s oddělenými tlačítky na ovládání nahrávání.

Vyskytne-li se poplach, vestavěný indikátor upozorní uživatele, že je nevyhnutelná jeho pozornost. KTD-405U uchovává až 32 polachů v chronologickém pořadí. První tři poplachy jsou na displeji a tón bzučáku bude znět každých 15 sekund, dokud nebudou potvrzeny všechny poplachy.

Obr. 9: KTD-405 zdroj:
http://www.gesecurityproducts.eu/CZ/products_single.php?product=KTD-405U

1.3.2.4 Digitální kamera KTC-815CP

Digitální kamery KTC-815CP patří do rodiny statických kamer společnosti GE Interlogix. Jedná se o barevnou digitální kameru s vysokým rozlišením a právě to je jejich velkou předností. Díky snadnému ovládání a nastavení jsou ideální pro použití tam kde je

požadována vysoká kvalita obrazu. Mají široký rozsah napájení a díky packu plus je možné jej připojit ke stávajícím sítím, tedy jsou plně kompatibilní. Jako detekční senzor je využíván Sony Super HAD CCD s rozlišením 795x596obrazových bodů, tedy nějakých 480TV řádků. Možnost i připojení různých objektivů v závislosti na využití.

Obr. 10: KTC-815CP zdroj: [15]

1.3.2.5 Otočná kamera CyberDome

Otočná kamera CyberDome, v tomto případě typ venkovní den/noc 25x je závěsná kamera s možností záběru velkého prostoru. Rychlost otáčení kamery je až 400°/s, s možností výběru z několika programovatelných režimů nebo přímého ovládání pomocí klávesnice KTD-405. Natáčení kamery umožňuje sledovat obraz v záběru až 360° horizontálně a 180° vertikálně. K dispozici je 25x optický zoom a 12x digitální zoom. Snímací senzor CCD s rozlišením 752x582pixelů standardu PAL s citlivosti 3lux barevně a 0,2lux černobíle. K přepínání mezi černobílým a barevným záznamem může dojít automaticky v závislosti na množství světla.

Obr. 11: Otočná kamera CyberDome

Zdroj: [15]

1.3.3 Elektronický požární systém

Vzhledem k současnému vývoji technologického vybavení budov se stále zvyšují požadavky na požární bezpečnost. Základem je předejít ztrátě na životech, újmě na zdraví a v neposlední řadě i škodám na majetku zapříčiněných vznikem a rozšířením požáru. Právě k těmto účelům je navržen samostatný protipožární systém. Jeho jediným účelem je detekce požáru, nejlépe ještě předtím než naplno propukne. Z chemického hlediska má průběh hoření několik fází. Kouřová čidla systému EPS jsou navržena tak, aby dokázala zachytit i první fáze a předala co nejrychleji zprávu ústředně. Tak pak v závislosti na předané informaci vyhodnotí situaci a zachová se dle předem nastavených možností. Kdy je nutné použít samostatný požární systém definuje zákon č.67/2001Sb. Jedná se především o objekty veřejně přístupné - Nákupní centra, divadla, hotely a knihovny. Systémy je možné instalovat i do neveřejných soukromých objektů, mnohdy ale vystačí kombinace systému Elektronického Zabezpečovacího Systému s kouřovými čidly.

Bohužel tahle budova je vybavena pouze nouzovými tlačítky pro případ požárů. Jediný detektor kouře je pouze v bezpečnostní místnosti v prvním podzemním podlaží. Kde je instalován i samo hasící systém.

1.3.4 Bezpečnostní rám METOR 160

Průchozí detektor kovu METOR 160 se vyznačuje bezchybnou funkčností, výrobce udává jen 5% nechtěných poplachů, a robustním provedením.vyznačuje se vysokou rovnoměrností detekce a rovnoměrností citlivosti po délce rámu. Je řízen mikroprocesorem s možností nastavení několika režimů a zabezpečení přístupovým kódem pro znemožnění manipulace s ovládáním. Eliminuje okolní rušivé elementy a po detekci alarmu je schopný v krátkém časovém limitu pokračovat v činnosti. Možnost připojení ovládání může být z větší vzdálenosti. Zobrazuje kovové předměty pomocí audiovizuálních efektů. LED indikátory znázorňuji umístění a velikost předmětu.

Obr. 12: METOR 160, zdroj: http://www.mercotrade.cz

2 SOCIOTECHNICKÝ AUDIT

Bezpečnost informačních systémů není pouze záležitostí technickou, velmi významným prvkem bezpečnosti je i lidský prvek. Lidské chování je rozmanité a lidským chybám nejde úplně zabránit. Největší nutnost je počítat se selháním lidského faktoru. Lidským selháním jde zabránit vhodným nastavením systému, Takovým problémem se zabývá sociální inženýrství. Potřebujeme-li získat nějaké informace o nějaké osobě, firmě nebo organizaci, můžeme postupovat různě. V případě bezpečnosti informačních systémů se často hovoří spíš o sledování sítí, nabourávání se do systémů zvenčí, ale existují i mnohem jednodušší a méně náročné praktiky.

Mezi časté netechnické způsoby útočníků patří dnes tzv. sociotechniky, které využívají lidských slabin v jednání. Sociotechnika jako jeden s pojmů bezpečnosti je přesvědčování a ovlivňování lidí s cílem oklamat je tak, aby uvěřili, že útočník je někdo jiný a zmanipulovat je k vyzrazení informací nebo provedení určitých úkonů. Při těchto metodách se útočník pokusí pomocí manipulace přesvědčit oběť, aby prozradila nějakou významnou informaci. Např. heslo je sděleno neznámému, kdo se představí jako správce systému, po telefonu nebo vloženo na podvržený formulář apod. Další metodou sociotechniků je získání původně zcela nevinné informace, ze které si pak útočník odvodí nějakou informaci významnější. Často mají organizace na svých stránkách řadu informací, které při vhodně kombinaci mohou vést ke získání údajů pro tuto firmu či organizaci životně důležitých, které by jinak tajila. Proto, pokud sociotechnik chystá na nějakou organizaci útok, začne právě studiem internetových stránek, odkud získá jména, internetové adresy, případně telefony pracovníků firmy, šéfů atd. Pak je možno pokračovat i na osobní stránky těchto lidí, kde jsou opět někdy zajímavé informace. I když je totiž v bezpečnostní politice dané organizace nějak zajištěno, co smí a nesmí být na firemních stránkách, již obvykle nikdo nezjišťuje, co má daný člověk na svých soukromých stránkách, s čím vstupuje do diskusí na internetu atd. A zdaleka ne všichni jsou alespoň natolik obezřetní, aby měli různé přezdívky, přihlašovací jména a adresy pro různé účely. Další, co může být pro útočníka zajímavé, je vnitropodniková terminologie, utajená telefonní čísla, kód vnitropodnikového útvaru apod. Proto by mezi základní bezpečnostní opatření mělo patřit provedení auditu stránek organizace, zjistí se, zda neobsahují zbytečné údaje, zda tam vývojář nenechal nějaké zbytečné informace. Dále je nutno dbát na to, aby informace, které jsou vhodné pro intranet, nebyly zbytečně umísťovány na internetu. Např. v loňském roce prováděla jedna moje diplomantka podobný bezpečnostní audit

nejmenované organizace, resp. jejích webových stránek. Např. zde našla informace o tom, jak je v dané organizaci vytvářen login resp. způsob odvození uživatelského jména, dále zde zjistila, jaký software používají servery, apod. Zkrátka je dobré dohlédnout na to, zda informací poskytovaných veřejnosti není zbytečně moc. I z informací na první pohled nevinných může útočník získat něco vhodného pro sebe. K těmto metodám se dá vlastně také počítat tzv. trashing, kdy se prolézají skutečné odpadky nejenom virtuální (prolézání firemních odpadů, za účelem nalezení dokumentů o struktuře sítě, jmen pracovníku, hesel atp.). Po získání základních informací je možno přistoupit k samotnému útoku, třeba získat po telefonu nějaké významné informace. Nejsnazší útok je ve velké organizaci, kde se lidé navzájem nezdají a kde je možno třeba zavolat novému zaměstnanci a přes něj se pokusit získat informace. Sociotechnik mu zavolá, přivítá ho jako nového pracovníka ve firmě a začne např. s bezpečným nastavením hesla a připojením k síti. Nový pracovník je nadšený tím, že se zde o něj tak dobře starají, a udělal by skoro cokoliv. Navíc i pokud bude mít nějaké podezření, tak si přece na novém pracovišti nebude hned dělat problémy. Ideální jsou velké organizace, kde se může útočník vydávat za pracovníka sice ze stejné firmy, ale jiné pobočky, ústředí atd. Pamatuji, kterak na jedné konferenci povídal zajímavý příběh pracovník auditorské firmy, která mj. prováděla bezpečnostní audit v nejmenované bance. Tento pracovník byl fingovaně najat do banky (se souhlasem vedení) a kromě jiných pokusů o útok obvolal vybrané pracovníky s tím, že je nutno změnit heslo, které jim bylo nadiktováno po telefonu. Poté obešel všechny, kterým volal a zjišťoval, kolik lidí si změní heslo na jiné, které jim kdosi neznámý (leč jistě vystupující ve vhodné roli) nadiktuje. Dle jeho líčení to byla zhruba polovina lidí, ovšem ostatní si heslo nezměnili hlavně kvůli tomu, že to nedovedli, ne že by nechtěli. Sociotechnici se často ptají na zdánlivě nezajímavé, nedůležité informace, které nedávají žádný smysl, ale pak je postupně poskládají dohromady a pokusí se o úspěšný útok. Mohu jen pozdvihnout obočí nad chováním jisté významné banky, ze které mi již několikrát volala paní (ovšem kdo ví odkud skutečně byla) a snažila se mi vnutit jakousi kartu (zlatou, stříbrnou, diamantovou, puntíkatou či jakou) a její hovor začínal otázkou, jaký mám plat. To skutečně pracovnice příslušného oddělení čeká, že ji budu po telefonu vykládat informace o mém platu? Pokud to ale čeká, tak se asi najdou lidé, kteří to udělají. Dalším z tahů k oklamání lidí je získat si jejich důvěru (např. Dobrý den, já jsem ten a ten z oddělení xxx a pracuji s Jardou a Honzou, znáte Honzu? Říkal mi, že se mu moc líbíte…) oběť věří útočníkovi, že zná jejího kamaráda Honzu, protože útočník si získal i další informace z Honzova života, takže mu

bude plně důvěřovat. Důležité také je, aby oběť neměla příliš času na přemýšlení. Proto obvykle sociotechnici naléhají na důležitost daného úkonu, nebo na časovou tíseň, takže se oběť nezamyslí ani nad důsledky daného úkonu a spíš bude útok úspěšný. Další způsob je ovlivňování lidí pomocí autority: pokud například sociotechnik na oběť naléhá, že je to pro jejího šéfa a už to dávno mělo být hotové, tak chudák sekretářka ze strachu udělá, co se jí řekne. Někteří lidé jsou velmi povídaví a ve vhodném prostředí vyzradí kde co. Velmi dobře si vzpomínám na situaci, kdy jsem čekala na letišti v Helsinkách na letadlo do Prahy. Vedle mne sedící dva obchodníci si sdělovali natolik důvěrné obchodní informace o právě uzavřeném obchodu, že by jistě šlo tyto informace vhodně zpeněžit. Nějak je vůbec nenapadlo, že na přímý let do Prahy může třeba čekat někdo další, kdo mluví česky. Způsobů, jak útočit na lidskou hloupost, neznalost, ješitnost apod je mnoho, jedním z nejnovějších a zároveň velmi nebezpečných útoků využívajících sociotechniky je tzv. phishing. Jedná se o velmi závažnou hrozbu, o které nejsou běžní uživatelé informováni a která využívá lidské naivity až hlouposti, takže obrana je velmi složitá.

Většina autorů, kteří se zabývají socitechnikami, udává těchto šest základních lidských vlastností, které se dají použít pro sociotechnický útok. Je proto při jakémkoliv jednání mít podobné techniky sociotechniků na paměti a počítat s nimi.

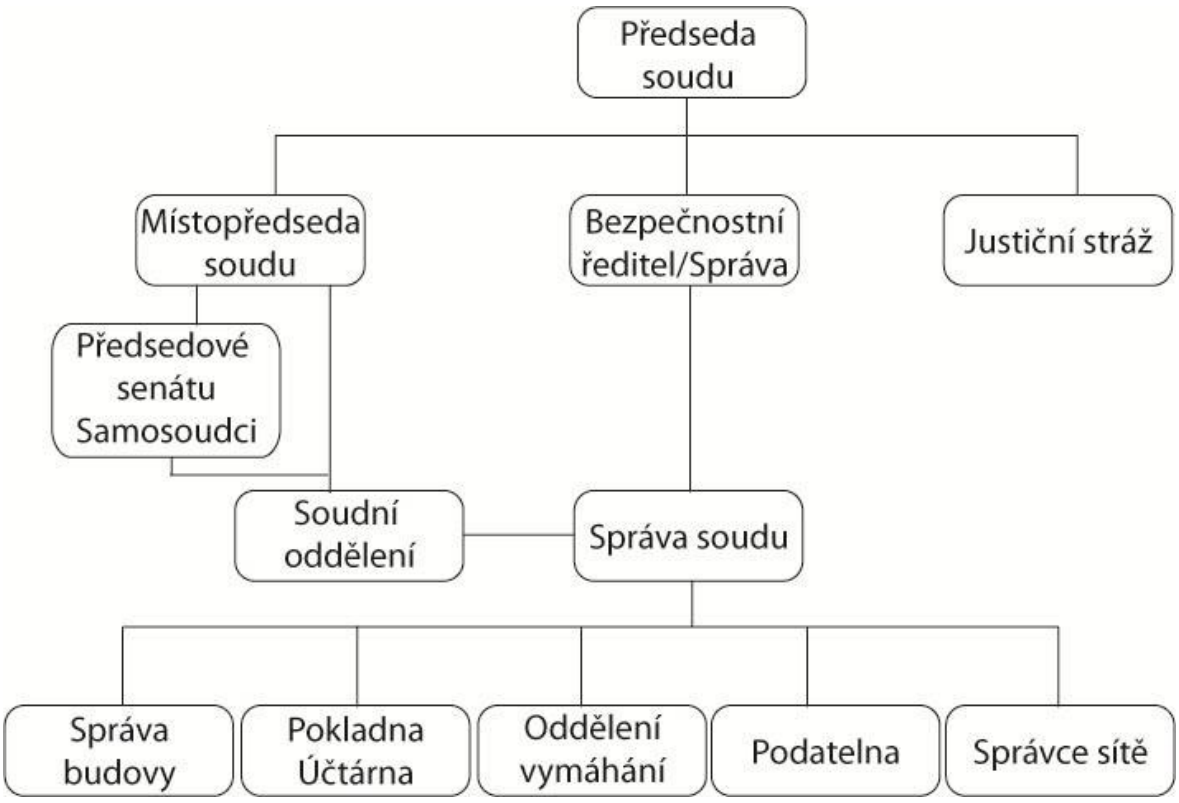
- **Autorita** – lidé mají tendenci se podřídit osobě s větší funkcí (mocí). Jedinou obranou proti tomuto je dodržování určitých bezpečnostních pravidel všemi a pracovník, který odmítne podat informace třeba řediteli firmy, pokud tento nemůže prokázat identitu, nesmí být potrestán (ale právě naopak). Z hlediska bezpečnosti by si měli být všichni rovni.
- **Sympatie** – sociotechnik může získat sympatie oběti několika způsoby: stejné názory, zájmy, sport atd. Pokud sociotechnik získá sympatie případné oběti, pak od ní může získat příslušné informace.
- **Vzájemnost** – je mnohem větší pravděpodobnost, že sociotechnikům oběť vyhoví, když pro ní předtím něco udělají. Například sociotechnik nejprve vyřeší problém se sítí (i třeba imaginární) a pak řekne oběti, ať si nainstaluje program, který bude síť hlídat, což přitom ve skutečnosti může být trojan, keyscan atp. Obranou je opět dodržování bezpečnostní politiky ve všech situacích.
- **Důslednost** – lidé mají tendenci se podřídit, jestliže předtím veřejně vyhlásili svou podporu a angažovanost v určité záležitosti.

- **Společenský souhlas** – sociotechnik zavolá a zeptá se zda-li nemá oběť čas, že by potřeboval vyplnit dotazník, který už všichni ostatní s ním vyplnili.
- **Vzácná příležitost** – viz posílání mailů. Tohoto způsobu využívá kdekdo: prvních 100 vyhrává, byl jste vylosován (nakonec zjistíte, že tzv. vylosováni byli všichni). Jenom vyplňte Vaše údaje atd.

2.1 Jednotlivé skupiny justičních zaměstnanců

Zaměstnance nebo spíš pracovník soudu nebo státního zastupitelství můžeme rozdělit dle různých struktur. Nejlepší rozdělení by bylo dle mého názoru na dvě skupiny. Tou první by byly zaměstnanci soudu neboli ministerstva spravedlnosti pod kterou spadají. Jednalo by se vlastně o soudce, státní zástupce, čekatele, zapisovatelky, překladatele a další pracovník přímo pracující na výkonu úkolů daných zákonem o ustanovení soudů a soudní moci. Tou další větší skupinou bych viděl samotnou Justiční stráž, která sice taky spadá pod Ministerstvo spravedlnosti, ale zajišťuje spíše zabezpečení daných objektů a ochranu soudních zaměstnanců. Z různých pohledu docházíme k určitým propojováním jednotlivých kategorii a jejich členění. Proto si pro názornou ukázku provedeme rozčlenění dle budovy Okresního soudu, viz. Obrázek níže.

Problematika dle sociotechnické oblasti je u každé struktury různá, protože zde dochází ke styku s utajovanými informacemi, popřípadě informace o bezpečnostním systému daného objektu. Ale přesto se zaměříme spíše na členy Justiční stráže z hlediska zabezpečení objektu. Protože soudci, státní zástupci a další osoby, dostávající se od styku s utajovanými skutečnostmi se řídí určitými stanovami a etickými kodexy jak s takovými informacemi nakládat. Následně by se to dalo shrnout na samostatnou práci, pokdu bychom měli vystihnout všechny aspekty sociotechnické auditu.



Obr. 13: Členění administrativy, zdroj. Vlastní

2.1.1 Justiční stráž a její povinnosti

Justiční stráž vykonává strážní službu v prostorách soudu a státních zastupitelství. Je zřízena a řízena Ministerstvem Spravedlnosti prostřednictvím generálního ředitelství pro vězeňskou a justiční stráž. Její hlavní činností je zajištění bezpečnosti v budovách soudu a státních zastupitelství. Provádějí kontrolní činnost jak na daných stanovištích (vstupech do budovy) tak obchůzkovou činností po daném objektu. Součástí jejich práce je i zajištění bezpečí soudců a jednotlivých zaměstnanců, musí být v případě zavolaní schopni ihned řešit mimořádné události. Velkým rizikem je vzhledem k sociotechnickému auditu u těchto lidí, znalost celé budovy včetně bezpečnostního systému a jeho slabých míst. Všeobecná pravidla pro justiční stráž na okresních soudech mohou vypadat například takto:

1) *Nevpustí do budovy soudu osobu, u níž se technickými prostředky, prohlídkou zavazadla nebo vozidla, osobní prohlídkou nebo jiným zjištěním přesvědčí, že má u sebe střelnou zbraň nebo jiný předmět, kterým může ohrozit život a zdraví osob, nebo se takovéto prohlídce odmítne podrobit. Jedná-li se však o osobu předvolanou*

k soudnímu jednání, informuje o této skutečnosti předsedu určitého senátu, který osobu předvolal, dále se řídí jeho pokyny.

2) *Zajistí uložení předmětů ohrožujících život a zdraví osob, pokud není stanoveno pokynem předsedy okresního soudu jinak. Musí vyplnit stanovenou dokumentaci.*
3) *Sleduje chování a činnost osob zdržujících se v blízkosti strážního stanoviště a v případě jejich podezřelého jednání nebo chování neprodleně informuje velitele místní jednotky justiční stráže a dále se řídí jeho pokyny.*
4) *V případě podezření na protiprávní jednání osob na tomto strážním stanovišti, které by mohlo ovlivnit bezpečný průběh soudního jednání nebo jiné činnosti okresního soudu, oznámí tuto skutečnost veliteli místní jednotky justiční stráže.*
5) *Pravidelně kontroluje funkčnost, neporušenost a úplnost mechanických zábranných prostředků a provádí potřebná opatření k odstranění zjištěných nedostatků.*
6) *Při předvádění osob do soudní budovy za účelem uvalení vazby informuje předvádějící orgány PČR o přítomnosti a činnosti osob, které svým jednáním daly najevo, že mají vztah k předváděné osobě, nebo projevily zájem o předváděnou osobu.*
7) *Při příjezdu a odjezdu eskorty Vězeňské služby ČR nebo PČR spolupracuje s velitelem eskorty s cílem zajištění bezpečného průchodu eskorty soudní budovou do eskortní místnosti popřípadě do jednacích síní. Při plnění těchto úkolů úzce spolupracuje s ostatními strážními stanovišti.*
8) *Všechny případy nevpuštěných osob do budovy okresního soudu a jejich důvod ihned oznámí veliteli místní jednotky justiční stráže.*
9) *Má přehled o osobách vstupujících se střelnou zbraní do budovy soudu (například příslušníci bezpečnostních sborů), nebo se v budově například pohybují příslušníci vězeňské služby, nebo policie.*
10) *Při velkém množství osob vstupujících do budovy soudu, za předpokladu, že nezvládne danou situaci a do budovy by mohla být vnesena střelná zbraň nebo nebezpečný předmět, uzavře hlavní vchod a požádá velitele místní jednotky justiční stráže o posílení, poté do budovy soudu vpustí jen takový počet osob, který lze důkladně zkontrolovat.*
11) *Nedovolí odkládání zavazadel, balíčků a jiných předmětů v prostorách hlavního vchodu do budovy soudu. Nalezení některých z výše uvedených předmětů ihned hlásit veliteli místní jednotky justiční stráže.*

12) *Monitoruje pohyb tělesně a duševně postižených osob a případně jim zajistí fyzickou pomoc při bezbariérovém přístupu do budovy okresního soudu a jejich prostor.*
13) *Při rádiovém provozu dodržuje hovorovou kázeň, používá stanovené volací znaky a radiostanici využívá pouze ke služebním hovorům.*
14) *Stanoveným způsobem podává hlášení kontrolním a jiným funkcionářům Vězeňské služby České Republiky.* [7]

II. PRAKTICKÁ ČÁST

3 INOVACE POPLACHOVÝCH A ZABEZPEČOVACÍCH SYSTÉMŮ

Neustálý vývoj nových technologii v oblasti zabezpečení a nejen v ní. Nás vede k zjištění, že i při aplikaci nejmodernějších bezpečnostních systémů je bude nutné po určité době obnovit nebo nahradit novými. Velmi často dochází při nových zařízení k jejich optimalizaci, protože až uvedení do praxe ukáže úskalí některých vlastností. Samozřejmě to neznamená každý rok nebo dva velké investice do systému zabezpečení, ale najít optimální dobu po které provedeme novou analýzu celého prostoru a zhodnotím zda použité zařízení je stále dostačující. Protože po určité době může dojít ke změnám různých aspektu mající vliv na zabezpečený prostor.

3.1 EZS a CCTV

Aktuální zabezpečovací systém je postavený na výborném základu a i když má už nějaké roky za sebou, stále bych jej zařadil mezi ty lepší. Ale i zde se dá najít spousta úskalí a prostoru ke změně. A navíc vývoj nikdy nezastavíš. Předně mě zaráží nepropojení některých systémů. V příkladu instalované kamery řady KTC společnosti GE a jejich ovládací systém disponují detekcí pohybu a i když je v budově instalováno určité množství PIR čidel, viděl bych propojení kamerového systému s poplachovým za docela rozumnou cestu. Takový postup by eliminoval určitá úskalí, například falešné poplachy, a navíc by neměl vliv na samotnou funkci jednotlivých systémů. Ale to už je záležitost při finálním návrhu systému, a dá se kdykoliv do budoucna zakomponovat.

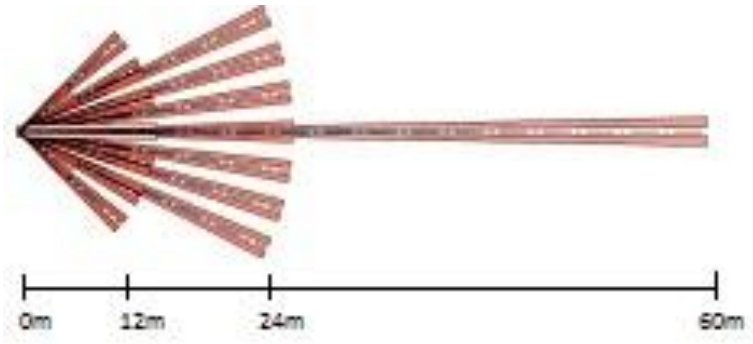
Samotný poplachový systém bych zanechal na daném základu a to ústředně ATS4000, která je svými kvalitami stále mezi tím nejlepším co můžeme na trhu najít. I když si prošla za ty roky určitým vývojem. Hlavní úpravou, kromě výše zmiňované propojení systémů, bych viděl přidání venkovního PIR detektoru, kvůli lepší ochraně chráněného prostoru kolem budovy. Aktivní detektor rozbití skla kvůli eliminaci falešných poplachů na stávajících detektorech při každém zatřepání okna. Magnetické kontakty na všech oknech a dveřích plní svou úlohu na výbornou a není důvod je měnit. Pro změnu u CCTV systému bych udělal radikálnější změnu. Vytipováním bych některé kamery vyměnil za kvalitnější s možností nočního vidění. Alespoň u venkovních bych tak učinil s nastavením střeženého prostoru na daný perimetr, jako základ pro ochranu vně objektu.

3.1.1 Modifikace technologie EZS a CCTV

3.1.1.1 Detektor EV630

Pasivní infračervené detektory řady EV630 jsou kombinací vysoké úrovně zabezpečení s nejvyšší možnou úrovní odolnosti proti falešným poplachům. Jejich velkou předností je variabilní charakteristika snímání s dosahem až 60m. Dokonalá teplotní kompenzace a možnost činnosti v prostředí od -18°C do +50°C a vlhkosti až 90%.Paměť prvního a každého dalšího poplachu, i možnost ověření tzv. programovatelným zdvojeným hlídačem („Double Checker“). Dále také využití režimu o očí do očí s dalším detektorem a spoustu perimetrických nastavení. Byl schválen pro použití v objektech s vyššími riziky certifikátem NBU a pro použití i v objektech Armády ČR. Spojením všech těchto faktorů je ideální pro použiti ve venkovním prostoru.

Obr. 14: Pasivní infračervený detektor EV630 zdroj: http://www.efg.cz/



Obr. 15: Možnosti pokrytí EV630 zdroj: http://www.efg.cz/

3.1.1.2 ShatterPro II

Akustický detektor rozbití skla ShatterPro II se může pyšnit certifikátem NBÚ-D. Nabízí detekci tříštění sklad rozšířenou až na poloměr 7,5m. Tato povrchově montovaná jednotka rozezná tříštění sklad v plném rozmezí 360° a následně provádí verifikační test. Možnost detekce i skrz neprůhledné nebo světlé záclony. Tříštění skla detekuje napříč celým frekvenčním spektrem, i díky tomu je schopná detekovat tiché nebo opatrné rozbíjení skla. Vhodná pro všechny typy skel včetně vrstveného, laminovaného, temperovaného a drátěného.Svůj stav indikuje i pomocí vestavěné LED diody a při instalaci není nutná žádná kalibrace zařízení díky citlivému mikrofonu. Možnost práce v prostředí od -18°C po + 50°C.

Obr. 16: ShatterPro II zdroj: [15]

3.1.1.3 Kamera TIR-600

Jedná se o barevnou bezpečnostní kameru z řady výrobku GE se snímačem CCD o možnosti 330 TV řádků. Vybavena technologii pro den a noc s možností automatického sepnutí vestavěné infračerveného LED podsvícení. Vyznačuje vysokou citlivost a flexibilnosti co se umístění týká. Citlivost se pohybuje od 0,5lux až po 0lux při využití IC LED podsvícení. Velikost objektivu je 6mm a celá kamera je umístěna v pouzdře splňujícím požadavky IP68. Efektivní vzdálenost snímání při využití LED se pohybuje kolem 10m.

Obr. 17: IC kamera TIR-600 zdroj: [15]

3.1.1.4 Otočná kamera LEGEND

Legend je nová, otočná dome kamera od GE Security, která využívá špičkové technologie SilkTrak™ přímého řízení pohybu. SilkTrak™ eliminuje rázy vznikající při pohybu kamery, která jsou typickým prvkem vetšiny kamer s mechanickými převody a pohonem. Prostřednictvím grafického menu můžete nastavovat jednotlivé trasy, makra, otáčení, v závislosti na poplachových vstupech, nebo prostě jen natočení kamery na jednotlivé pozice. Mezi její velké přednosti patří technologie den a noc kdy je schopná při přepnutí na technologii ICR pořizovat záznamy již při 0,01lux. Kamera je vybavena CCD snímačem při rozlišení 460TVL PAL. Disponuje 26x optickým zoomem a 12x digitálním zoomem. Samozřejmosti je i množství programovacích úkonů, jako snímané trasy, hlídané zóny, maskované oblasti.

Obr. 18: Otočná kamera Legend zdroj: [15]

3.2 Elektronická požární signalizace

EPS neboli elektronická požární signalizace je systém hlídající nebo spíš eliminující riziko rozšíření požáru. Skládá se tak jako EZS z aktivních nebo pasivních členů které buď při detekci sami spustí alarm nebo zašlou informaci ústředně, která jej spustí, popř. ještě zašle informaci na PCO. Jak jsme zjistili z analýzy objektu, není zde daný systém integrován, až tedy na jednu místnost se spisy. Vzhledem ke stávající úloze daného objektu si myslím, že by bylo logické implementovat systém EPS. Ať již z důvodu pohybu velkého počtu lidí, nebo vybavení, tak i s ohledem na práci s utajovanými skutečnostmi, popřípadě jinými důležitými předměty nebo materiály.

Při návrhu systému bych zavrhl možnost implementace EPS do stávající zabezpečovacího systému, ačkoli ústředna ATS4000 by takovou možnost umožňovala. Důvod je prostý, v případě výpadku nebo havárie centrálního systému, by došlo i k ochromení systému EZS a to by bylo vzhledem k důvodům instalace elektronické požární signalizace nežádoucí. Proto daný systém navrhuji se samostatnou řídící ústřednou, která samozřejmě může doplňkově zasílat informace systému EZS. Na následujících nákresech je rozmístění jednotlivých prvků.

3.2.1 Technologie EPS

3.2.1.1 Ústředna FP1216EN

Analogová adresovatelná požární ústředna, 2 kruhové smyčky, lze rozšířt až na 4 kruhové smyčky, indikace 16 zónových LED na panelu, pro střední a větší systémy. Na displeji je v češtině zobrazen kompletní údaj o situaci v systému. Systém nabízí několik mechanizmů, které výrazně zvyšují odolnost celého systému EPS proti falešným poplachům, hlavně automatickou kompenzaci hodnot pozadí, dvojí aktivaci a koincidenci uvnitř zón a mezi nimi. Obsluha je ústřednou upozorněna na nutný servisní zásah jakmile některý z hlásičů dosáhne prahu zaprášení. Neocenitelnou pomůckou pro servis je kompletní statistika a diagnostika pro každou adresu, kterou lze získat buď z displeje LCD, nebo dálkově pomocí modemu. Ústředna nabízí mimořádné možnosti pro řízení V/V systému včetně implementace logických funkcí. Provázáním pomocí sítě je konfigurovatelná jakákoliv standardní kombinace požárních opakovačů a univerzálních uzlů pro připojení počítače. Programování pomocí PC (Upload / Download) je místní a nebo dálkové. Ústředna je kompatibilní s požárními hlásiči řady 2000 i 950. Komunikace s požárními hlásiči a současně jejich napájení je zajištěno dvěma vodiči. K ústředně je možné pomocí 2vodičové sítě ARCNET připojit požární opakovače. Nejideálnější aplikací ústředny FP1216EN je jejího využití pro výrobní organizace, sklady, hotely a úřady. Je kompatibilní s produkty řady FP2000 určené pro nejrozsáhlejší systémy. Možnosti jejího zapojení jsou na následujícím obrázku.

Obr. 19: Možnosti zapojení FP1216EN

zdroj: http://www.efg.cz/Produkty-Pozarni-signalizace-Stredni-systemy

Obr. 20: Ústředna FP1216EN zdroj: [15]

3.2.1.2 DP2061 Opticko-kouřový požární hlásič

Opticko-kouřový analogový požární hlásič je vybaven vyměnitelnou optickou komorou a výstupem pro paralelní signalizaci požáru. Detektory mají příjemný vzhled. Jednotlivé hlásiče jsou na sběrnici identifikované podle adresy, která se nastavuje dvěma otočnými přepínači. Adresou je číslo v rozsahu 1 -128 nastavované v desítkové soustavě, takže není potřebná konverze z dvojkové nebo šestnáctkové soustavy, což značně redukuje riziko nesprávné adresace. Optické hlásiče mají odnímatelnou optickou komoru, což umožňuje servis a čištění přímo na instalaci. Všechny hlásiče se montují na jednotnou montážní základnu DB2002, čímž se zjednodušuje objednávání.

Variantou je základna s izolátorem – DB2016. Řada 2000 obsahuje bohaté příslušenství. K dispozici jsou izolátory, jednotky na spínání sirén, zónové monitory a množství různých vstupních a výstupních modulů. Také je dostupná kompletní série tlačítkových hlásičů. Montážní základna s integrovaným izolátorem DB2016 zjistí a elektricky izoluje úsek kruhové linky se zkratem. Žlutá LED indikuje zkrat. Hlásič v základně s izolátorem bude v

případě jednoho zkratu stále napájen. Když je takovou paticí s izolátorem vybaven každý hlásič na kruhové lince, potom v případě jednoho zkratu žádný z hlásičů nepřestane fungovat.

Mezi jeho výhody patří:

- Možnost dálkového testu
- Možnost pripojit externí signalizaci
- Optický detektor s vymenitelnou optickou komorou
- Jednoduché numerické adresování (1-128)
- Vylepšený komunikacní protokol
- Kompletní automatická diagnostika
- Nezávislé na polarite
- Kompletní serie: optické a teplotní hlásice
- Kompletní nabídka V/V jednotek a príslušenství
- Základna s izolátorem
- Schváleno EN 54
- Schválení VdS
- Schválení v CR (TZUS)

Obr. 21: Opticko-kouřový požární hlásič DP2061 zdroj: [15]

3.2.1.3 Tlačítkový analogový hlásič DM2010

Adresovatelný tlačítkový požární hlásič DM2010 pro systémy požární signalizace je vyrobený z velmi pevného plastu a poplach je vyvolán rozbitím tenkého skla na jeho

přední straně. LED indikace zabezpečuje vizuální potvrzení poplachu ústřednou. Testovací klíč (dodávaný s každým kusem hlásiče) umožňuje otestování hlásiče bez rozebírání krytu. DM2010 je kompletní sada tlačítka, sklíčka a základny pro povrchovou montáž.

Vlastnosti:

- Analogový adresovatelný tlacítkový hlásic
- Rychlá odezva na aktivaci
- LED indikace požáru
- Sklícko a základna jsou v sade
- Obsahuje také testovací klíc
- Rychlý test s automatickým resetem
- Varianta DM2010E - IP67 pro venkovní aplikace

Obr. 22: DM2010 zdroj: [15]

4 OPTIMALIZACE SYSTÉMU ZABEZPEČENÍ

Na základě zjištěných skutečností díky provedeným analýzám jsme zjistili určité nedostatky v daném systému zabezpečení. Ale popravdě, žádný systém není natolik dokonalý, aby jej nebylo možné obejít. V předchozí kapitole jsme si nastínili možnosti úprav a změn z hlediska technických aspektů daného objektu. A i když by se mohlo zdát, že se jedná o zbytečné nebo banální změny. Můžou tyto změny v budoucnu docílit zkvalitnění systému zabezpečení v daném objektu. Samozřejmě je s tím spojená i určitá investice do modifikace takového systému. Ale jak nám analýza ukázala je možné využít velké části stávajících prvků a tím náklady rozumně snížit.

4.1 Zabezpečovací systém

Základem systému zabezpečení v budově sídla Justice se stane zabezpečovací ústředna ATS 4000 od společnosti GE Interlogix, kterou je v závislosti na použitých modulech možné využit jako drátovou i bezdrátovou. Tato ústředna již je součástí objektu. K použité ústředně ATS4000 ještě využijeme ústřednu FP1216EN od stejné společnosti pro systém elektronické požární signalizace. Její pořizovací cena se pohybuje kolem **38.000,-Kč+DPH**

Díky určitému zaměření dané budovy si můžeme rozdělit jednotlivé prostory do dílčích kategorií s uvedením systému zde použitého.

Prostor Chodba:

- Discovery DUO-AM, PIR a MW detektor, počet 2x-3x, již nainstalován
- Magnetické čidlo otevření MK440, počet v z. na oknech a dveřích, již nainstalován
- Kamera TIR-600 s IC technologii, počet 1x, cena cca **20.000,-Kč+DPH**
- Tlačítkový hlásič DM2010 vnitřní, počet 3x, cena **1.300,-Kč/ks+DPH**
- Opticko-kouřový požární hlásič DP2061, počet 2x, cena **1.500,-Kč/ks+DPH**
- Detektor rozbití skla ShatterPro II (7,5m) , počet 1x, cena **2.000,-Kč/ks+DPH**

Jednací místnost:

- Discovery DUO-AM, PIR a MW detektor, počet 1x, již nainstalován
- Magnetické čidlo otevření MK440, počet v z. na oknech a dveřích, již nainstalován
- Kamera TIR-600 s IC technologii, počet 1x, cena cca **20.000,-Kč+DPH**
- Opticko-kouřový požární hlásič DP2061, počet 1x, cena **1.500,-Kč/ks+DPH**
- Detektor rozbití skla ShatterPro II (7,5m) , počet 1x, cena **2.000,-Kč/ks+DPH**
- Tíšňové NO/NC tlačítko ART476, počet 1x, již nainstalováno

Kanceláře:

- Discovery DUO-AM, PIR a MW detektor, počet 1x, již nainstalován
- Magnetické čidlo otevření MK440, počet v z. na oknech a dveřích, již nainstalován
- Opticko-kouřový požární hlásič DP2061, počet 1x, cena **1.500,-Kč/ks+DPH**
- Detektor rozbití skla ShatterPro II (7,5m) , počet 1x, cena **2.000,-Kč/ks+DPH**

Podatelna:

- Discovery DUO-AM, PIR a MW detektor, počet 1x, již nainstalován
- Magnetické čidlo otevření MK440, počet v z. na oknech a dveřích, již nainstalován
- Kamera TIR-600 s IC technologii, počet 1x, cena cca **20.000,-Kč+DPH**
- Opticko-kouřový požární hlásič DP2061, počet 1x, cena **1.500,-Kč/ks+DPH**
- Detektor rozbití skla ShatterPro II (7,5m) , počet 1x, cena **2.000,-Kč/ks+DPH**
- Tíšňové NO/NC tlačítko ART476, počet 1x, již nainstalováno

Skladovací místnost:

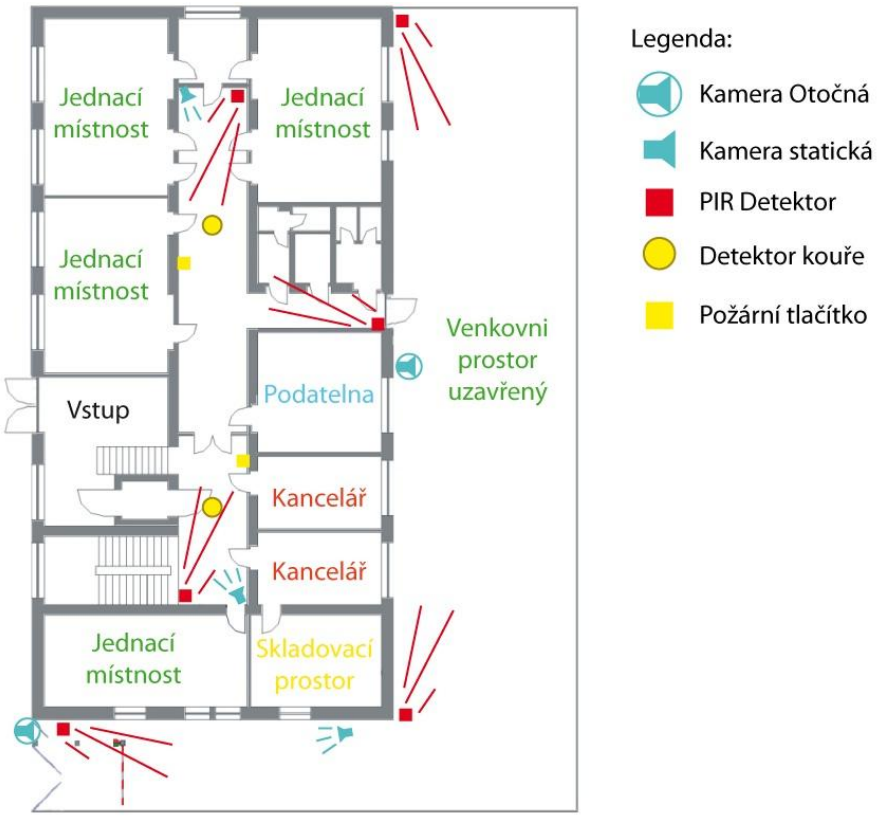
- Discovery DUO-AM, PIR a MW detektor, počet 1x, již nainstalován
- Magnetické čidlo otevření MK440, počet v z. na oknech a dveřích, již nainstalován

- Opticko-kouřový požární hlásič DP2061, počet 1x, cena **1.500,-Kč/ks+DPH**
- Detektor rozbití skla ShatterPro II (7,5m) , počet 1x, cena **2.000,-Kč/ks+DPH**

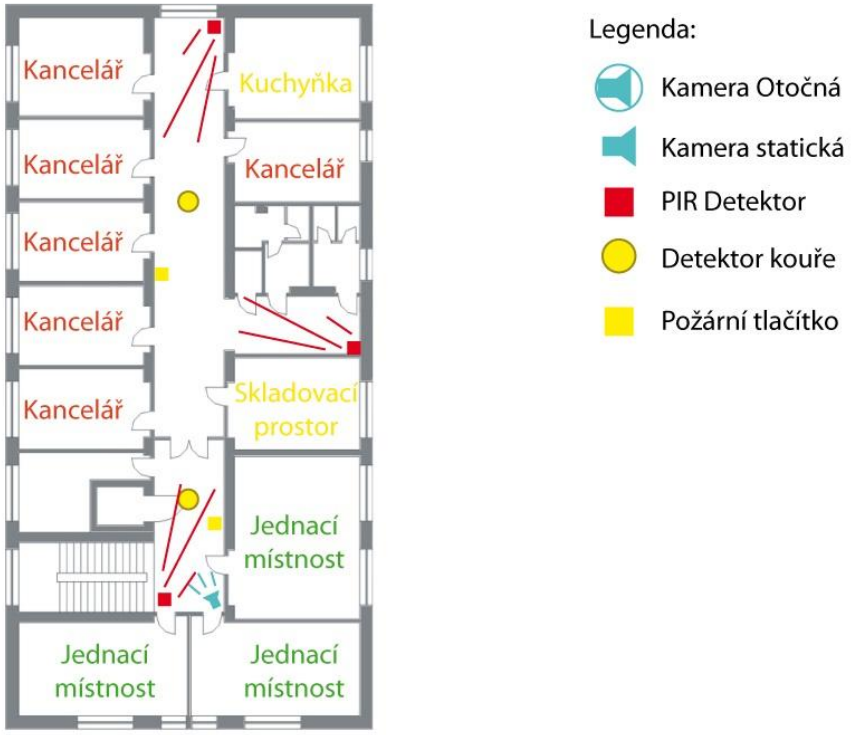
Venkovní prostor:

- Otočná kamera LEGEND s tech. Noc/den, počet 2x, cena cca **25.000,-Kč/ks+DPH**
- PIR detektor EV630, počet 2x, cena cca **2.000,-Kč/ks+DPH**
- Kamera TIR-600 s IC technologii, počet 1x, cena cca **20.000,-Kč+DPH**

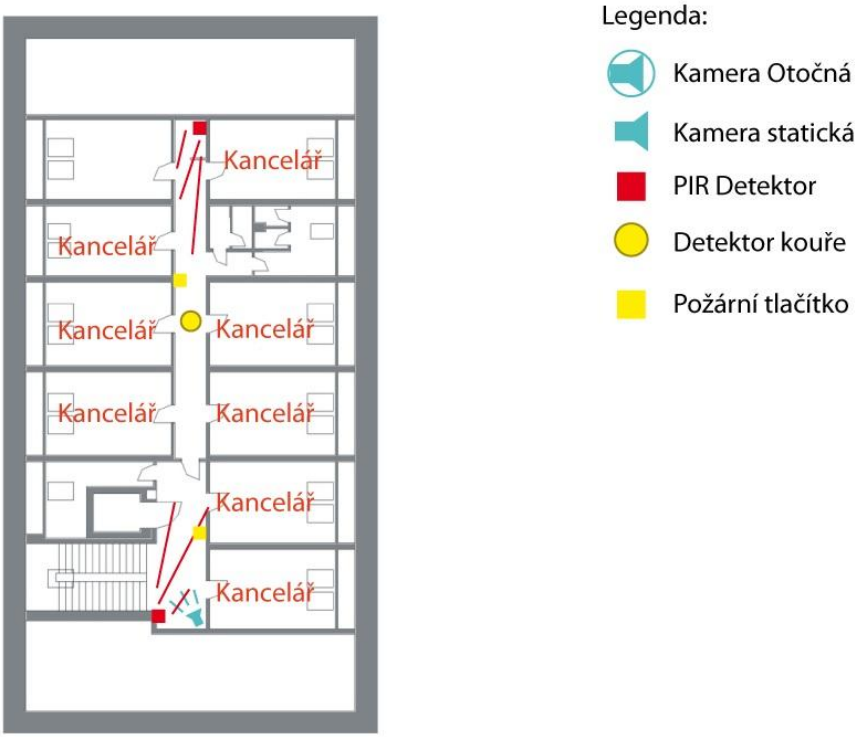
V seznamu nejsou zahrnuty další instalační prvky, jako kabely, komunikační prostředky u některých zařízení a další prostředky potřebné pro instalaci. Uvedení zabezpečení vstupu a k nim příslušných prostor není uvedeno záměrně, zabývá se jimi samostatná kapitola. Na následující nákresech je označeno umístění prvků, z bezpečnostních důvodů jsou místnosti označeny pouze názvem pro spojeni se seznamem.



Obr.23: 1. nadzemní podlaží – zakreslení, zdroj: vlastní



Obr.24: 2. nadzemní podlaží – zakreslení, zdroj: vlastní



Obr.25: 3. nadzemní podlaží – zakreslení, zdroj: vlastní

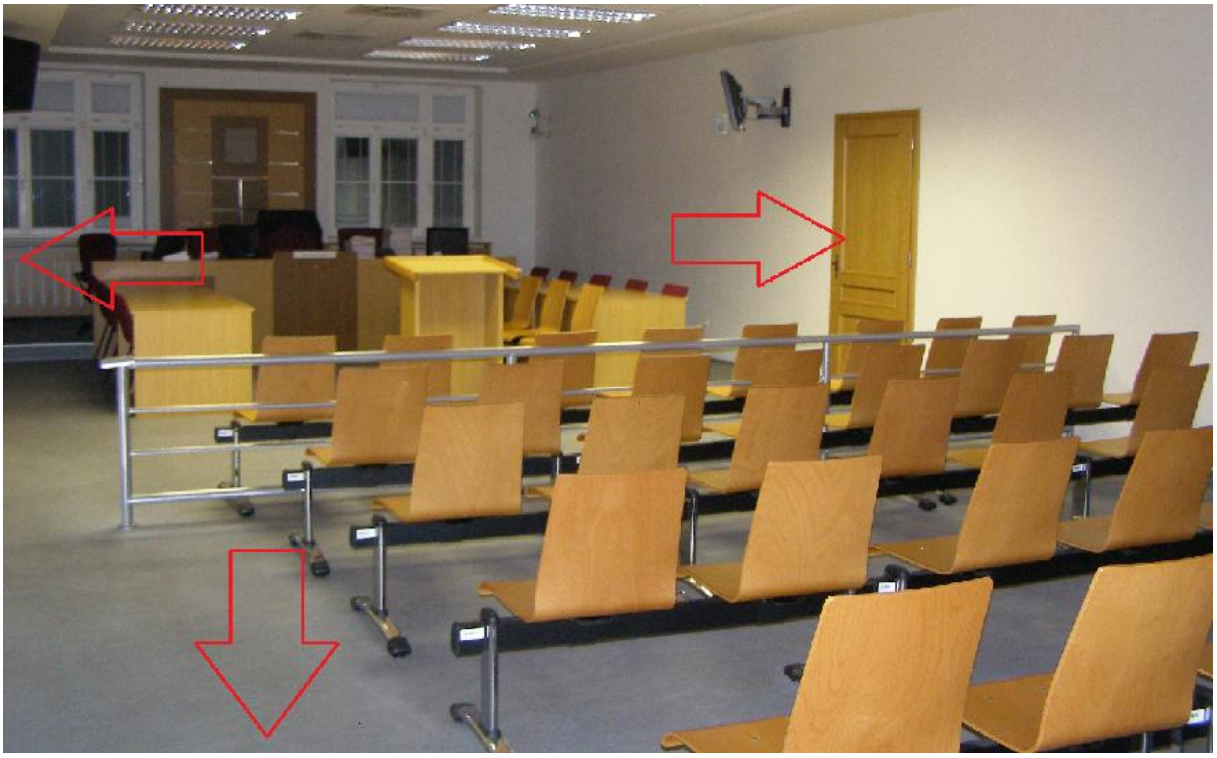
4.2 Vstupy a únikové východy

Na okresních soudech jsem se nejvíce zaměřil na únikové cesty z jednacích síní a vedoucích pracovišť jako i kanceláře soudců a jejich rychlostí vyklizení a to hlavně při napadení budovy, nebo při vzniku požáru, který by šlo jen velmi špatně eliminovat a to z důvodu velkého množství spisového materiálu, který bývá zpravidla uložen ve sklepech těchto soudních objektů.

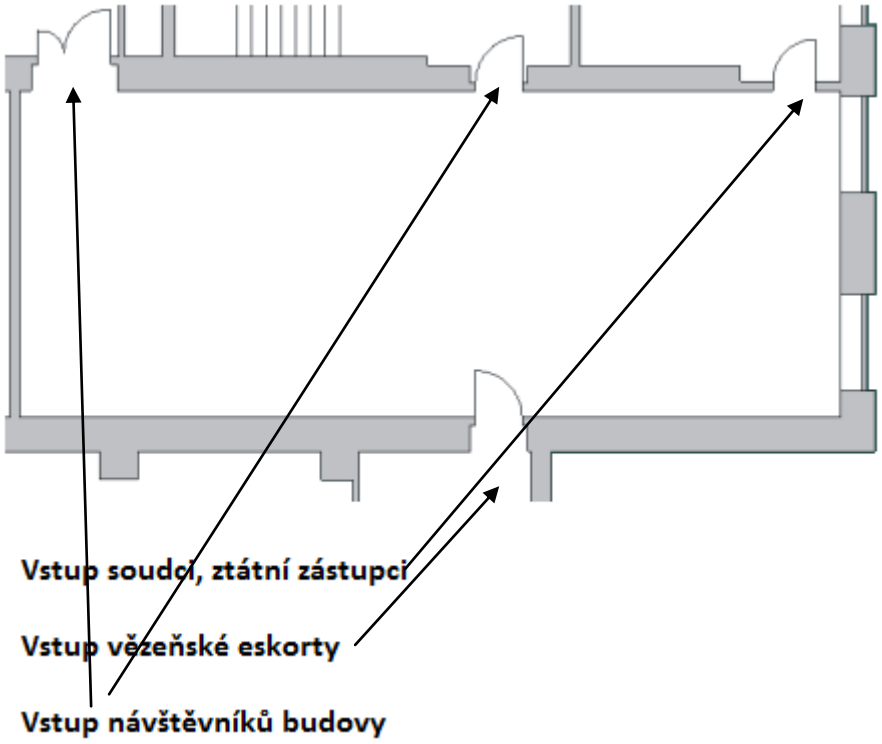
Obr. 26: Ilustrace spisovny zdroj: vlastní

4.2.1 Jednací síně

Zajištění jednacích síní je velmi dobře uzpůsobeno jak při napadení tak i při vzniku požáru a to v jakémkoli místě jednací síně a to z toho důvodu, že většina jednacích síní má několik vstupů, zpravidla se jedná o tři vstupy, které slouží pro návštěvníky soudu, soudce a státní zástupce, popřípadě advokáty a soudní znalce a poslední ze vstupů je pro vězeňskou eskortu.



Obr. 27: Jednací síň – únikové východy zdroj: vlastní

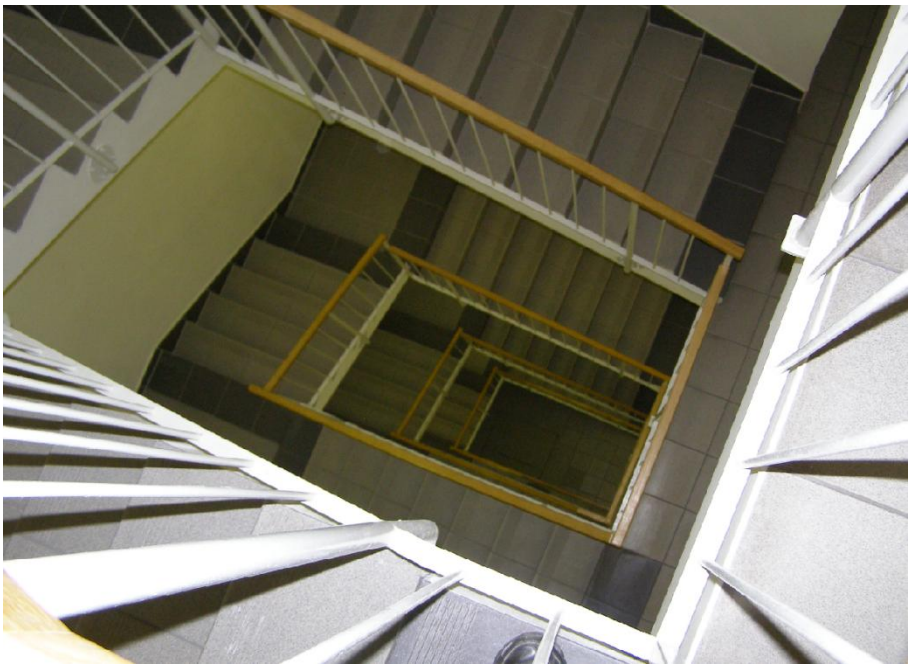


Obr. 28: Jednací síň-zakreslení zdroj: vlastní

Z tohoto důvodu jsem neviděl co by jsem mohl na únikových východech v jednacích síních měnit. Únikové východy jsou velmi dobře uspořádány a vyklizení těchto jednacích síní by bylo velmi rychlé a to z toho důvodu, že při nastání mimořádné události jako je například požár mohou návštěvníci soudu opustit tyto prostory přes jakýkoli východ, krom východu vězeňské služby pokud právě probíhá jednání s eskortou vězeňské služby.

4.2.2 Únikové východy ostatních pracovišť

Při zkoumání únikových východu z ostatních pracovišť okresního soudu jsem narazil na velmi závažný problém a to z toho důvodu, že jedna z konkrétní budovy okresního soudu má pouze jedno schodiště a je rozvržena do třech pater. Při požáru na schodišti, by nikdo nemohl z budovy okresního soudu uniknout.

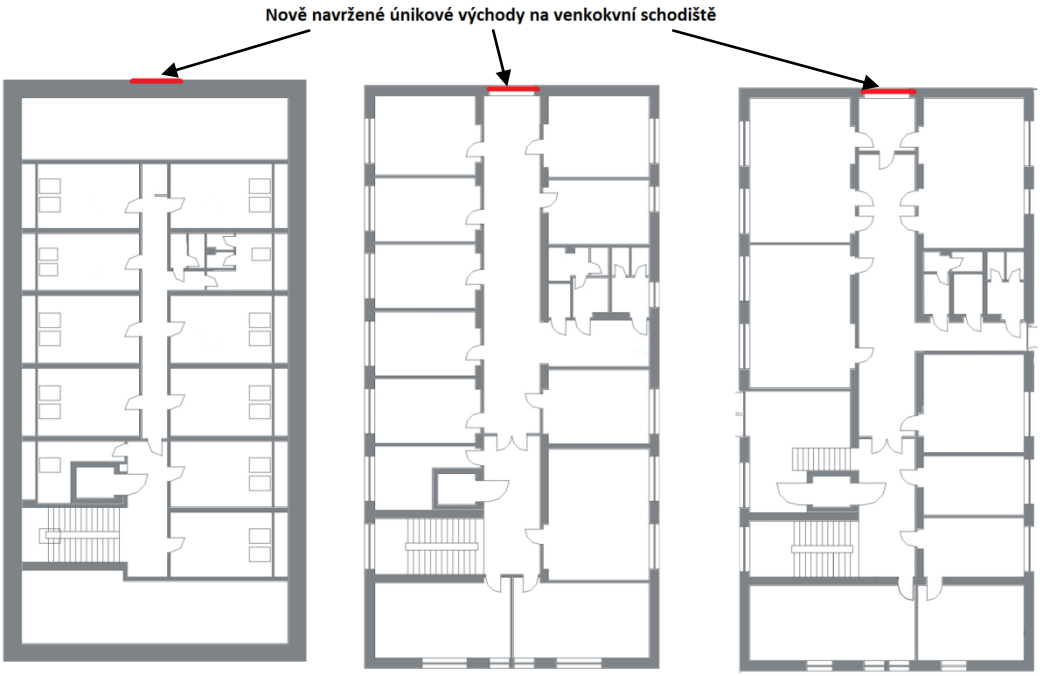


Obr. 29: Schodiště Zdroj: Vlastní foto

4.2.3 Navržené opatření

Na druhé straně každého podlaží jsem navrhnul venkovní únikový východ, který by umožnil bezproblémové opuštění této budovy při požáru schodiště jako je například na budově hotelu Continental v Praze.

Obr. 30: Ilustrace únikového schodiště Zdroj: www.Hotel_continental.cz



Obr. 31: Zakreslení umístění únikového schodiště Zdroj: Vlastní

Z toho důvodu, že se únikové schodiště stávají často zneužívané pro páchání trestné činnosti, jako jsou například krádeže, nebo napadení, každý z těchto vchodů jsem opatřil

magnetickými kontakty a kontrolním čidlem nouzového východu. Kontrolní čidlo nouzového východu NG má díky svému modulovému provedení flexibilní možnosti použití a nejvhodnější je při použití u různých dveřních konfigurací Sériově je čidlo vybaveno signálním zařízením s aktivací poplachu a čidlem, které spouští poplach při sejmutí krytu.

Kontrolní čidlo kontroluje nouzové východy budov a vydává akustické zvuky v případě, že dojde k jejich otevření.

Pro provozovatele budovy je důležité poznat, zda jsou nouzové východy uzavřené a zabezpečené nebo zda jsou otevřené. Kvůli častému zneužití nouzových východů je nezbytné provádět jejich kontrolu přídavným zařízením. Kontrolní čidlo nouzového východu Vás jako provozovatele okamžitě informuje akustickým poplašným zvukem, pokud dojde k otevření nouzového východu – ať jde o únik nebo nedovolené otevření. Kontrolní čidlo východu slouží také jako zábrana neoprávněného otevření. Toto poplašné zařízení se používá především v nákupních centrech, hotelech, nemocnicích, školách, školkách, správních budovách i ve veřejných objektech.

Bezpečnostní znaky:

- Zařízení funguje na baterie, není nutná kabeláž
- Vhodné pro plnostěnné nebo profilové rámové dveře, pro dveře s panikovým madlem nebo ve spojení s bezpotenciálovým spouštěčem alarmu
- Oprávněná osoba může provést nastavení a zrušení do pohotovostní polohy nebo odstranit kryt schránky
- Ochrana před manipulací a sabotáží

Obr. 32: Kontrolní zařízení únikového východu

zdroj: www. evva.cz/ access to security.htm

ZÁVĚR

V dané diplomové práci, jsem vzhledem k požadavkům a pokynům pro zpracovaní, zhodnotil stávající stav zabezpečení sídla justice. Zaměřené hlavně na zabezpečovací systémy, jako jsou EZS, CCTV, EPS. Zpracováním analýzy rizika a zhodnocení technických prostředků. V případě elektronických zabezpečovacích systému nebyly shledány žádné problematické aspekty, avšak vzhledem k určité době již provozovaného systému a zjištěni různých problémů během provozu, jsem navrhl určitou obměnu některých prvků tohoto systému. V případě zaměření se na CCTV systém shledávám jako nedostatek nepropojení systému se systémem EZS. Vzhledem k investicím, které byly do systému vloženy při jeho realizaci a technologickým možnostem jednotlivých prvků. Bych řekl, že je škoda nevyužit výhod a vlastností obou systému pro zvýšení míry zabezpečení a snížení rizika. CCTV systém totiž nemusí sloužit jen čistě ke sledování určité oblasti pracovníkem ostrahy nebo pořizováním záznamu, může se stát i aktivním členem celého systému zabezpečení.

Jako hlavní nedostatek mi přišla absence protipožárního systému u takového objektu. Kdy jsme z analýzy objektu zjistili, že jediný použit prvek EPS je pouze v místnosti se spisy a dokumenty. Proto jsem zpracoval návrh možné implementace systému EPS do objektu. V základě se jedná o instalaci detektoru kouře a tísňových tlačítek na chodbách a v jednotlivých místnostech. Cely systém jsem navrhl jako samostatný funkční prvek s vlastní řídící a vyhodnocovací jednotkou, jen s propojení na aktuální systém a pultem centrální ochrany. Vždyť dnes takový systém používá řada domácností ve větších domech, proto si myslím, že u objektu s větším výskytem osob by měl být základem. Chceme přece chránit zdraví lidí, majetek a další věci mající nějakou cenu, proto bychom měli myslet na jejich bezpečnost i z pohledu mimořádných událostí bez účasti cizí osoby.

Dalším bodem bylo zhodnocení vstupů a únikových východů, z praktického hlediska jsem se zaměřil právě na ty únikové východy. Rozdělením dané problematiky do různých kategorii nastínilo dva různé pohledy na danou problematiku. V případě vstupu do jednotlivých místností, které zároveň slouží jako únikové bych nadnesl jejich výborné řešení. I když v případě místnosti pro utajované svědky mě překvapil její přístup z prostoru pro čekatele na dané jednání, ale tím bych se teď nezabýval. Spíš mě zaujala možnost jen dvou únikových východů z budovy, což by ještě bylo dostačující. Ale pouze jedno schodiště v celé budově a výtahy, které se v přípravě vzniku mimořádné události vypnou.

Nemyslím si, že je dostačující pro evakuaci osob ve veřejné budově mít možnost využít pouze jedné únikové cesty z vyšších pater. V návaznosti na danou skutečnost a stavební indispozice dané budovy, jako i vyšší náklady na realizaci stavby dalšího schodiště, jsem navrhl přistavění schodiště ze železné konstrukce. Nové schodiště by bylo zvenku připojeno na objekt a sloužilo by pouze pro případ evakuace osob.

V závěru bych rád podotkl, že již nyní používaný systém je z hlediska funkčnosti dostačující. Ale navržené optimalizace a úpravy by zvýšilo efektivnost bezpečnosti sídla justice.

ZÁVĚR V ANGLIČTINĚ

In this thesis, I am due to requirements and guidelines for processing, reviewed the current security status of the seat of justice. Focused mainly on security systems, such as intrusion detection, CCTV, electronic fire systems. Processing risk analysis and evaluation of technical means. In the case of electronic security system have found no problematic aspects, however, due to a period of time operating system and various problems detected during the operation, I proposed a variation of some elements of the system. In the case of focusing on the CCTV system as I find the lack of an unrelated system, intrusion detection system. Given the investments that were entered into the system during its implementation and technological capabilities of individual elements. I would say it is a pity untapped advantages and features of both systems to increase the level of security and risk reduction. CCTV system is not used purely to monitor certain areas of security personnel or acquisition record, it can also become an active member of the security system.

As a major flaw I came to the fire system in the absence of such an object. When we found the object of analysis, the only element of fire is used only in the room with the writings and documents. So I prepared a possible implementation of fire to the building. The basis is to install smoke detectors and emergency buttons in the hallways and individual rooms. The whole system I designed as a single functional element with its own control and evaluation unit, with only links to the current system and ARC. For such a system now used by many households in larger houses, so I think that the object with a higher incidence of persons should be the basis. We want to protect human health, property and other items having a price, therefore we should think of their safety from the perspective of emergency without the participation of foreign persons.

Another point was to evaluate the entries and emergency exits, from a practical standpoint, I just focused on the escape exits. Dividing the problem into different categories outlined two different perspectives on the issue. In the case of entry to individual rooms, which also serves as an escape I raised them an excellent solution. Although in the case of classified rooms surprised me seeing her approach from space for the trainee to act, but by now I would not deal with. Rather, I was intrigued by the possibility of only two emergency exits from the building, which would still be sufficient.

But only one staircase in the building and elevators that are in the preparation of emergency shut down. I do not think it is sufficient to evacuate people in a public building be allowed to use only one means of escape from upper floors. Following the construction and the fact indisposition of the building, as well as higher costs of implementing further building stairs, I proposed delivery of the iron staircase design. The new staircase would be connected from outside the object, and would serve only in case of evacuation.

In conclusion I would like to say that it is already used by the system is sufficient in terms of functionality. But the proposed optimization and adjustments would increase the effectiveness of the safety seat of justice.

SEZNAM POUŽITÉ LITERATURY

[1] KŘEČEK, Stanislav. Příručka zabezpečovací techniky. Vyd. 2. S.l.: Cricetus, 2003, 351 s. ISBN 80-902-9382-4

[2] FRIEDMAN, George. The intelligence edge: how to profit in the information age. 1st ed. New York: Crown, c1997, 276 s. ISBN 06-096-0075-3.

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

[4] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management I. 1. vyd. Zlín: VeRBuM, 2011, 316 s. ISBN 978-808-7500-057

[5] VYMĚTAL, Dominik. Informační systémy v podnicích: teorie a praxe projektování. 1. vyd. Praha: Grada, 2009, 142 s. ISBN 978-802-4730-462

[6] ŠTĚDROŇ, Bohumír. Manažerské řízení a informační technologie. 1. vyd. Praha: Grada, 2007, 156 s. ISBN 978-802-4720-524

[7] Vězeňská služba České Republiky, Pravidla pro výkon služby justiční stráže u vchodu do budovy soudu, 1996

[8] Instrukce MSp č.j. 500/2002-SOBŘ, kterou se vydávají zásady zabezpečení justičních objektů,

[9] Instrukcí MSp č.j. 95/2002 SOBŘ , o zabezpečení utajovaných skutečností zpracovávaných informačními systémy v resortu MSp

[10] Zákon č. 412/2005 Sb., ochraně utajovaných informací a o bezpečnostní způsobilosti

[11] Zákon č. 413/2005 Sb., o změně zákonů v souvislosti s přijetím zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti

[12] Zákon č. 555/1992 o Vězeňské službě a justiční stráži ČR,

[13] Instrukcí MSp č.j. 60/2006-OBKŘ o justiční stráži,

[14] Bezpečnostní odbor MV ČR: Pomůcka k problematice zajišťování bezpečnostní ochrany objektů, Praha: MV ČR, 2012

[15] GE Security. [online]. [cit. 2012-02-15]. Dostupné z: www.gesecurity.cz

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACS	Access kontrol system
AIR	Active Infra Red
CCD	Charged Coupled Device
CCTV	Close Circuit TeleVision
DS	Docházkový systém
EKV	Elektronická kontrola vstupu
EPS	Elektrická požární signalizace
EZS	Elektronický Zabezpečovací Systém
HZS	Hasičský záchranný sbor
LCD	Liquid Crystal Display
LED	Light Emitting Diode
MW	MicroWave
MZS	Mechanické zábranné systémy
OPPO	Obslužný panel požární ochrany
PCO	Pult Centralizované ochrany
PIR	Passive Infra Red
SHZ	Stabilní hasící zařízení

SEZNAM OBRÁZKŮ

SEZNAM TABULEK