Návrh přístupového systému pro konkrétní budovu místní samosprávy

Design Access System for the Specific Building of Local Government

Bc. Leona GABRIELOVÁ

Diplomová práce
2013

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2012/2013

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Leona Gabrielová**
Osobní číslo:	**A11388**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Návrh přístupového systému pro konkrétní budovu místní samosprávy**

Zásady pro vypracování:

1. **Popište současná řešení přístupových systémů a jejich možností.**
2. **Popište stávající systém, zpracujte současné organizační schéma a režimová opatření objektu.**
3. **Analyzujte slabá místa v systému.**
4. **Navrhněte nové organizační schéma, režimová opatření.**
5. **Navrhněte technické prostředky pro zajištění požadovaných funkcí.**
6. **Vytvořte kritéria pro hodnocení dodavatelů systému.**
7. **Vyhodnoťte přínos.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **ČSN EN 50133. Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011. Třídící znak 334593.**
2. **ŠENOVSKÝ, Michail, BALOG, Karel. Integrální bezpečnost. 1. vyd. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2009, 104 s. ISBN 978-80-7385-076-0.**
3. **KŘEČEK, Stanislav a kol. Příručka zabezpečovací techniky. 2. vyd. Blatná: Blatenská tiskárna, 2003, 351 s. ISBN 80-902938-2-4.**
4. **UHLÁŘ, Jan. Technická ochrana objektů II. díl – Elektrické zabezpečovací systémy II. 1. vyd. Praha: Policejní akademie ČR, 2005, 229 s. ISBN 80-7251-189-0.**
5. **UHLÁŘ, Jan. Technická ochrana objektů III. díl – Ostatní zabezpečovací systémy. 1. vyd. Praha: Policejní akademie ČR, 2006, 246 s. ISBN 80-7251-235-8.**
6. **LUKÁŠ, Luděk a kol. Bezpečnostní technologie, systémy a management I.. 1. vyd. Zlín: Verbum, 2011, 316 s. ISBN 978-80-87500-05-7.**

Vedoucí diplomové práce: **Ing. Rudolf Drga**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **8. února 2013**

Termín odevzdání diplomové práce: **3. června 2013**

Ve Zlíně dne 8. února 2013

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Předmětem této diplomové práce je návrh přístupového systému pro budovu místní samosprávy malého města. Teoretická část se zabývá přístupovými systémy obecně, dále pak zabezpečovacími systémy a možnosti rozšíření přístupových systémů o systémy docházkové. Praktickou část tvoří již samotný přístupový systém vypracovaný na základě konkrétních potřeb s návrhem režimových opatření a technických prostředků včetně požadavků kladených na dodavatele těchto systémů.

Klíčová slova:

Přístupový systém, přístupová práva, bezpečnost, režimová opatření, docházkový systém.

ABSTRACT

The subject of this assignment is to design an access system for a building of a small town authorities. The theoretical part deals with access systems in general, with security systems and the options as how to get the attendance into such access systems. The practical part pays attention to the access system itself. It is developed based on specific needs with draft mode measures and technical means, including requirements for suppliers of these systems.

Keywords:

Access control system, access rights, security, routine measures, attendance system.

Poděkování

Děkuji Ing. Rudolfu Drgovi za odborné vedení, mnoho cenných rad, připomínek a podnětných konzultací, kterými přispěl k vypracování této diplomové práce. Současně chci poděkovat také mojí rodině a přátelům za trpělivost a podporu při studiu.

Motto

„Pokrok nespočívá v tom, včerejšek zbořit, ale zachovat jeho podstatu, která má sílu stvořit lepší dnešek.“

Jose ORTEGA Y GASSET

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové 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 práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové 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 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 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 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 práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové 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

V oblasti bezpečnosti jsou kladeny zvyšující se nároky na ochranu; stále více se zaměřujeme na bezpečnost osob, majetku a také na ochranu informací. Tato skutečnost se ve velké míře také týká bezpečnostních aplikací a systémů, které přichází do styku s těmito informacemi. Informační systémy mohou být rozsáhlé a řešit tak celou škálu požadovaných úloh (přístupy, evidence, sklad, účetnictví, řízení) nebo naopak mohou být zaměřeny pouze na jeden konkrétní problém. Řadíme mezi ně také přístupové systémy, které sice majetek nechrání přímo, ale umožňují omezení přístupu do zabezpečených prostor, kontrolu přístupu osob a určování přístupových práv.

Elektronický přístupový systém (ACS) nahrazuje klasické klíče všude tam, kde je třeba identifikačním systémem zabezpečit vstup do budovy nebo přímo do konkrétní místnosti dané budovy. Identifikační systém okamžitě rozpozná oprávněnou osobu a umožní či zamítne vstup, a to například po přiložení čipu k přístupovému terminálu nebo otiskem prstu, jedná-li se o kontrolu pomocí biometrických údajů. ACS umožňují v přehledném administračním rozhraní programu identifikačního systému jednoduché a pohodlné nastavení přístupu konkrétních zaměstnanců do určitých vyhrazených prostor. Systémy ACS jsou v nynější době na vysoké vývojové úrovni a při návrhu je důležité najít pro daný objekt takový systém, kde budou efektivně využity všechny jeho funkce.

Ve své diplomové práci jsem se rozhodla věnovat právě problematice návrhu přístupového systému pro konkrétní budovu místní samosprávy. Důvodem je také skutečnost, že v této budově pracuji, tedy znám reálné podmínky a mohu tak posoudit stav, výhody a nevýhody aktuálního řešení a současně mohu přispět k úpravě a vylepšení systému.

V teoretické části se nejprve krátce zabývám vývojem bezpečnosti v čase a postupným rozšiřováním požadavků na ochranu osob, majetku a informací. Dále se zabývám možnostmi ACS celkově pro možnost jejich zavedení či vylepšení stávajících systémů v administrativních budovách, tzn. v místech s vyšším pohybem osob a dále rozšířením těchto systémů o systémy docházkové. V praxi se mnohdy zaměňují pojmy přístupových a docházkových systémů. Věřím, že se mi v práci také podaří objasnit významy těchto systémů a jejich vzájemných vazeb. V praktické části se zaměřím již na určitý prostor s popisem jeho současného stavu; návrhem ACS s přihlédnutím ke konkrétním potřebám pro zvýšení bezpečnosti v budově, nynějším nedostatkům a současně s nástinem řešení slabých míst. Nezbytností je vypracování přehledného schématu uspořádání budovy

a možností pohybu určitých skupin osob po této budově. Dále tato část obsahuje návrh režimových opatření a technických prostředků, kterými se dá zabezpečit požadovaná funkčnost. V neposlední řadě jsou uváděna také kritéria pro hodnocení dodavatelů systémů a celkové vyhodnocení přínosu.

V dnešní moderní době se stále rozšiřují možnosti přístupu k sofistikovaným technologiím, zároveň však také sílí aktivity osob s protispolečenskými úmysly, které směřují od vandalismu až po ničivý terorismus. Řízení přístupů do budov se tedy stává nezbytnou součástí chodu jakékoliv společnosti.

Cílem mojí práce je návrh skutečně funkčního řešení ACS, kterým přispěji nejen k získání efektivního a uživatelsky elegantního systému, ale také dojde k zlepšení zabezpečení areálu nejen jak pro občany, kteří sem přicházejí vyřizovat své záležitosti, tak i pro zaměstnance samotné, kterým zajistí větší míru bezpečnosti a tím pádem přispěje k pocitu pohody a klidu na vykonávanou práci.

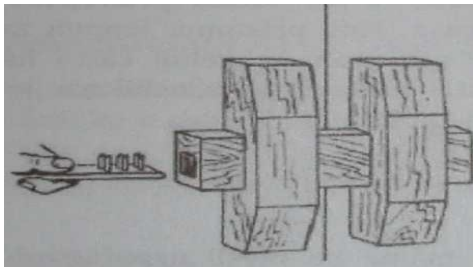
I. TEORETICKÁ ČÁST

1 OCHRANA OSOB, MAJETKU A INFORMACÍ

1.1 Vývoj zabezpečovacích systémů

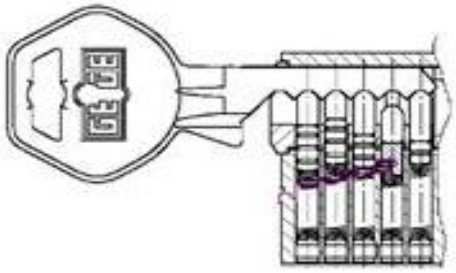
O ochranu majetku, osob a dalších hodnot se zajímají lidé od pradávna. S vývojem způsobu a podmínek života lidí, a především se změnou jejich životního stylu, se vyvíjely také způsoby zabezpečení majetku. Zajištění bezpečnosti v současné době nesporně vyžaduje komplexní a systémový přístup.

První mechanický zabezpečovací přístupový systém pochází ze starověkého Egypta. Byly to předchůdci dnešních zámků, tzv. egyptské dřevěné závory. Závory byly opatřeny systémem západek. Klíč představovala destička s kolíky, která se vsouvala do závory a nadzvedávala západky. Téměř všechny známé civilizace využívaly tento systém různě modifikovaný, do dnešní doby se zachoval v podobě cylindrické vložky. [9]



Obr. 1 Egyptská dřevěná závora [9]

V průběhu století a let se ve vývoji objevila celá řada mechanických zámků, vylepšovalo se jejich provedení i estetická stránka. S příchodem moderních, elektronicky řízených systémů se objevily také nové pojmy, které známe z dnešní doby.



Obr. 2 Současná dveřní vložka [18]

Cylindrická vložka je mechanismus, který je obvykle oddělený od příslušného zámku nebo západky a ovládá se klíčem. [11]

1.2 Požadavky na bezpečnost a její zajištění

Problematika bezpečnosti je velice široká. Je to pravděpodobně i tím, že člověk ke svému životu potřebuje bezpečnost, tedy alespoň většina z nás. Tak jak se poznání v průběhu let vyvíjelo, ruku v ruce s ním bylo lidstvo konfrontováno s novými, dříve nepoznanými riziky, se kterými se muselo a i do budoucna bude muset vypořádat. Se zvyšováním poznání se samozřejmě objevovala nová rizika, s tím i nutnost zabývat se těmito riziky, hledat cesty a možnosti jejich eliminace na únosnou míru. [12]

Snižování jakéhokoliv rizika je spojeno se zvyšováním nákladů, s nedostatkem znalostí, technických prostředků apod. Proto se v praxi hledá hranice, na kterou je únosné riziko snížit tak, aby vynaložené náklady byly ještě rozumné. Hovoříme o společensky ekonomické přijatelnosti rizika. Tato míra snížení rizika je většinou předmětem vrcholového managementu a politického rozhodnutí, při kterém by se měly využít současné vědeckotechnické poznatky a zohledňující se ekonomické, sociální a další podmínky.

Předmětem zájmu bezpečnosti každé organizace či podniku je ochrana osob, hmotného a nehmotného majetku. Bezpečnost je základní lidská potřeba. [21]

1.2.1 Bezpečnostní analýza

Před přijetím vážného rozhodnutí o chodu organizace či podniku je nutné zpracovat bezpečnostní analýzu. Bezpečnostní analýzu předchází činnosti bezpečnostního průzkumu a sběru informací z dostupných zdrojů. Provádíme ji při zjištění vážných nedostatků při ochraně objektu nebo před požadovanou změnou způsobu zabezpečení.

Analýza je jedním ze základních prvků konstrukce ochrany. [6] A pouze analýzou zjistíme efektivitu zabezpečení.

Hlavní předměty analýzy jsou obvykle objekty, subjekty (lidské zdroje), procesy, technika.

Obecná struktura analýzy:

- vyhodnocení minulého stavu,
- zjištění současného stavu,
- prognóza budoucího stavu. [7]

Analýza je pokus o získání objektivní pravdy o stavu zabezpečení organizace. [6]

Pro vytvoření analýzy rizik musíme nejdříve identifikovat aktiva a hrozby. Prvním krokem při identifikaci aktiv je zjištění, jaká aktiva se v systému vyskytují a jak jsou jednotlivá aktiva oceněna. Identifikace hrozby, která systém ohrožuje, se určuje v závislosti na prostředí, ve kterém bude systém nasazen.

Vlastní analýza rizik se provádí v posledním kroku, a to tak, že dojde k přiřazení konkrétních hrozeb konkrétním aktivům. Po provedení tohoto kroku by mělo být jasné, která aktiva ohrožují zanedbatelné hrozby a která je třeba naopak chránit.

1.2.2 Ostraha objektu

Ostraha objektu představuje klíčový prvek v oblasti aktivní bezpečnosti, tj. primární nárazníková oblast pro udržení pořádku v rámci zajišťované činnosti. Ostraha objektu sehrává velmi důležitou úlohu. [12]

Ochranu objektů (majetků, osob, informací) můžeme chápat jako soustavu vzájemně souvisejících preventivních opatření administrativního i výkonného charakteru, pomocí níž má být zajištěna bezpečnost zdraví a života pracovníků a návštěvníků objektu stejně tak jako ochrana majetku.

Pro potřeby této práce zmíním pojmy technické a elektronické ostrahy a režimového opatření. Jinak zde samozřejmě patří i **fyzická ostraha**, která je nejstarší formou zajištění pořádku a bezpečnosti, nicméně také tou nejdražší, protože ani s postupem času náklady na ni neklesají, spíše naopak.

Technická ostraha – jedná se o klasickou ostrahu a ochranu prostorů, míst a objektů pomocí technických prostředků. Jde o úplné využití elektrické a elektronické signalizace. Řadíme sem prostředky od mechanických zábranných systémů a prostředků přes elektrickou a požární zabezpečovací signalizaci, přístupové a docházkové systémy, uzavřené televizní střežící a dohlížecí systémy, ochranu dat a informací a biometrické identifikační systémy. [8]

Elektronická ostraha – jedná se o výkonnou efektivní ochranu majetku a osob. Využívá elektronických zabezpečovacích systémů, a to především PZTS, EPS, CCTV, ACS a různé havarijní systémy. Tyto systémy sledují objekt prostřednictvím speciálních detektorů, které zajistí včasnou signalizaci napadení objektu. Objekty se monitorují na dohledových a poplachových přijímacích centrech (DPPC) a je tak zajištěno permanentní střežení. Pokud

navíc kombinujeme s CCTV či s ACS, jde o ostrahu, kterou respektují všechny pojišťovací ústavy.

Režimová opatření – metoda ochrany osob a majetku, která využívá zavedení systému technicko-organizačních režimových opatření v objektu (vstupní propustky, časové a prostorové omezení, osobní omezení vstupu, vstup a výstup určitým prostorem, vydání režimových nařízení). Režimová ochrana je založena na zavedení a uplatňování účinných bezpečnostních směrnic, tzn. režimových opatření v chráněném objektu.

Režimová opatření představují stanovený soubor procedur, které zahrnují režim vstupu a výstupu osob, vjezdu a výjezdu dopravních prostředků, režim pohybu osob, dopravních prostředků a chráněných informací v objektu a jeho jednotlivých částech v pracovní i mimopracovní době, režim manipulace s klíči, identifikačními prostředky a médii, které se používají pro systémy zabezpečení vstupů, režim manipulace s technickými prostředky a jejich používání. RO jsou zpravidla popsána v provozním řádu objektu, zavazujícím všechny osoby, které jsou oprávněny vstupovat do objektu. Vedle jiných náležitostí obsahují RO i seznamy osob oprávněných vstupovat do chráněných prostorů objektu, seznam dopravních prostředků oprávněných vjíždět do objektu, způsob kontroly prokazování oprávněnosti k vstupu nebo vjezdu do objektu apod. [2]

Rozlišujeme tato režimová opatření:

- Vnější režimová opatření – týká se vstupních a výstupních podmínek, jde zejména o kontrolu vozidel a osob při vstupu a výstupu z chráněných prostor.
- Vnitřní režimová opatření – týká se pohybu uvnitř chráněného objektu; omezení pohybu vozidel a osob na určitém úseku chráněných prostor, zajištění osvětlení vybraných částí objektu, vytvoření signalizačních bariér při přiblížení k objektu.

Problematika managementu bezpečnosti v jakémkoli podnikatelském subjektu, ale také ve veřejné správě, není zcela jistě jednoduchou záležitostí.

1.3 Technické normy

Technické normy jsou předpokladem technického pořádku v daném oboru na příslušné úrovni, tedy např. celosvětově, mezinárodně, národně, v rámci určitého sdružení zájemců, podnikově, apod.

V oboru poplachových systémů začaly v posledním desetiletí 20. stolení vznikat na půdě evropských (CENELEC - Evropský výbor pro normalizaci v elektrotechnice) a světových (IEC - Mezinárodní výbor pro elektrotechniku) normalizačních organizací oborové standardy nabízející pro jednotlivé skupiny zařízení z oboru poplachových systémů. [5]

1.3.1 Normy pro systémy kontroly vstupu

Požadavky kladené na systémy kontroly vstupu v bezpečnostních aplikacích jsou stanoveny v souboru norem ČSN EN 50133. Tyto normy nemají závazný charakter, ale slouží především jako odkazové pro potřeby certifikace výrobků. V těchto normách jsou především stanoveny definice názvosloví a termínů, všeobecné funkční požadavky na systémy a komponenty, klasifikace stupně zabezpečení pomocí stanovení tříd identifikace a tříd přístupu. Dále jsou zde uvedeny definice a požadavky na třídy prostředí a třídy zařízení dle jejich umístění, mechanické, atmosférické a elektrické zkoušky zařízení, požadavky na elektromagnetickou kompatibilitu (EMC - schopnost zařízení fungovat vyhovujícím způsobem ve svém elektromagnetickém prostředí bez vytváření nepřípustného elektromagnetického rušení pro jiné zařízení v tomto prostředí), pokyny pro projektování, zřizování a provozování a požadavky na dokumentaci prováděcí, provozní, dokumentaci pro údržbu a revize). [9]

Norma popisuje všeobecné požadavky na funkčnost systému kontroly vstupů pro použití v bezpečnostních aplikacích. Norma také popisuje všeobecné požadavky na komponenty z hlediska prostředí. [3]

Nezbytnou podmínkou však je, že všechny prvky přístupových systémů musí splňovat požadavky na elektrickou bezpečnost (ČSN EN 60950, ČSN EN 60065), elektromagnetickou kompatibilitu a odolnost (ČSN EN 61000, ČSN EN 55022, ČSN EN 50082, ČNS EN 50130), případně požadavky telekomunikačních norem (např. ČSN EN 50529), v případě integrace s jinými systémy také ČSN CLC/TS 50398. *U prvků přístupových systémů musí být také samozřejmě prokázána shoda dle zákona č. 22/1997 Sb. a nařízení vlády č. 17/2003 Sb., o technických požadavcích na výrobky*

a č. 616/2006 Sb., o EMC kompatibilitě. [9] Požadavky na mechanické prvky přístupových systémů (otvírače, dveře, brány, turnikety) jsou uvedeny ve standardu Evropské komise CEN/TS 33. *Národní bezpečnostní úřad (NBÚ) vydal pro potřeby přístupových systémů a objektové bezpečnosti vyhlášku č. 339/1999 Sb.* [9] Souhrn zde uvedených norem, zákonů a vyhlášek není zdaleka vyčerpávající, není předmětem této práce.

Mezi poplachové systémy řadíme i Systémy kontroly a Systémy řízení vstupu (Access Control Systems). *Aplikace požadavků těchto norem je vymezena úlohou nasazení ACS v konkrétním objektu. V této oblasti probíhá neustálý vývoj na úrovni stále bezpečnějších a jednodušeji použitelných médií, jež jsou nositeli přístupového oprávnění. Principiálně je nutné počítat s aplikací požadavků vztahujících se obecně na informační systémy, rozhraní a začlenění ACS jako subsystému pracujícího na bázi přenosové sítě informačního systému nejen na úrovni hardwaru, ale i na úrovni softwaru.* [5] Nicméně bychom neměli zapomenout ani na požadavky v rámci požární bezpečnosti pro případy nutnosti evakuace osob z objektu, které s tímto úzce souvisí.

Jestliže některá část systému kontroly vstupů (SVK) tvoří část zabezpečovacího poplachového systému, musí tato část splňovat zároveň i příslušné požadavky norem na zabezpečovací systémy. Tato norma se zabývá zabezpečovacími aplikacemi pro každé přístupové místo. SVK se může skládat z libovolného počtu přístupových míst. [3]

1.3.2 Struktura norem přístupových systémů

Základní požadavky na poplachové systémy - systémy kontroly vstupů pro použití v bezpečnostních aplikacích jsou uvedeny ve skupinách evropských norem řady EN 50133+.

Tab. 1 Struktura norem skupiny ČSN EN 50133-x

Číslo normy	Název (zjednodušený)
EN 50133-1	Systémové požadavky
EN 50133-2-1	Identifikační zařízení - Všeobecné požadavky na komponenty
EN 50133-3	Vyhodnocovací zařízení
EN 50133-4	Výstupní ovládací prvek přístupového místa
EN 50133-5	Komunikace
EN 50133-6	Volná
EN 50133-7	Pokyny pro aplikace

2 PŘÍSTUPOVÉ SYSTÉMY

2.1 Vymezení pojmu

Přístupové systémy *řídí postup k chráněným prostorům, zařízením a informacím na základě jednoznačně deklarovaných přístupových práv.* [5]

Systém ACS nebo-li systém SKV můžeme chápat jako soubor opatření k zajištění řízení a evidence přístupu do zabezpečeného objektu nebo určitých prostor na základě jednoznačně přidělených přístupových práv. Daná opatření mohou být systémová, fyzická (fyzická ostraha), mechanická (mříže, zámky, závory) nebo elektronická. Kombinace systémů je samozřejmě nejúčinnějším řešením. Přístupová práva jsou pro každého uživatele přidělena na základě personální politiky, stupně oprávnění, časového harmonogramu, apod. Na základě přesné identifikace uživatele je po ověření přístupových práv povolen nebo zamítnut přístup. Sofistikovanější systémy umožňují například sledovat pohyb osob a jejich přítomnost v jednotlivých úsecích, definovat návaznost průchodů nebo měnit přístupová práva. [9]

Na úvod připomeňme, že musíme rozlišovat pojem „přístupový“ a „docházkový“ systém. Tyto pojmy se dosti často spojují v jeden, ale není to totéž. Obecně by se dalo říci, že docházkové systémy jsou podskupinou ACS.

Stejně jako u ACS, tak i u docházkových systémů je prokázání identity uživatele také nezbytné, ale prvotním cílem není pouze řízení přístupu do objektu, ale především monitorování času a důvodu průchodu daným místem (zákonná povinnost zaměstnavatele monitorovat pracovní dobu zaměstnanců, povinné přestávky a jiné důvody pro přerušení práce). Přístupové a docházkové systémy mohou být integrovány do jednoho celku s tím, že přístupových bodů je v objektu rozmístěno hned několik, zatímco docházkových bodů je obvykle mnohem menší počet (dosti často jen jeden u hlavního vstupu do objektu). [9]

2.2 Funkce přístupového systému

Jednou z hlavních částí bezpečnostních systémů jsou ty, které slouží k ověření identity osob. V této spojitosti je významným parametrem autentizace, tzn. ověření, zda je daná osoba skutečně tou, za kterou se vydává. Střežené objekty, kde je třeba monitorovat, evidovat nebo řídit přístup osob v souladu s jejich oprávněním, obvykle bývají rozděleny do **přístupových zón**. Přístupové systémy slouží k zpřehlednění pohybu vlastních

zaměstnanců i externích osob v zájmových prostorách a zajišťují obsluhu elektrického zámku dveří. Podle nastavených přístupových práv se dveře otevřou nebo neotevřou. Systémy bývají založeny na jednoznačné identifikaci osob. [1]

Mezi základní funkce přístupového systému podle T. Vítka a M. Husáka řadíme:

- identifikace,
- zpracování dat,
- styk s uživatelem (optické zobrazení, akustický signál),
- programovatelnost,
- ovládání přístupového místa,
- komunikace (s ostatními systémy nebo bloky přístupového systému),
- stavová hlášení,
- napájení systému nebo jednoho přístupového místa,
- samoochrana (ochrana proti sabotáži, neoprávněné manipulaci). [9]

Naopak Marek Čandík ve své knize Objektová bezpečnost uvádí tyto funkce:

- systém snímání průchodů – tvořen terminály pro monitoring průchodů a nebo řízení přístupů,
- přístupový terminál – specializované zařízení umísťované do nepřístupné oblasti uvnitř chráněné zóny,
- sledování stavu přístupových terminálů na monitorech,
- definování přístupových modelů – vytváření přístupových práv pro skupiny či jednotlivce,
- sledování průchodů přes zámky – ze zaznamenaných údajů lze sledovat a kontrolovat přítomnost vybraných osob v zadaném časovém intervalu,
- systém antipassback – systém pro hlídání opakovaných vstupů v jedné zóně; na každý vstup musí být výstup.

2.3 Přístupový bod

Přístupovým bodem v SKV rozumíme uspořádání všech prvků, které umožní kontrolovaný přístup v daném místě a tvoří jej:

- **místo přístupu** - zařízení, které umožní přístup (dveře, turnikety, brány),
- **rozhraní místa přístupu** - zařízení, které zajistí otevření a zabezpečení místa přístupu; řídicí jednotka obsahuje řídicí logiku, vstupy/výstupy potřebné k ovládání APAS, zajišťuje převod dat z identifikačního zařízení a komunikaci,
- **snímače místa přístupu** - identifikační zařízení, čtečka, klávesnice, biometrie,
- **APAS** - ovládací prvky a senzory přístupového místa; vstupní prvky - magnetické kontakty, spínače, optické závory (k signalizaci a zabezpečení místa přístupu), výstupní prvky - zámek, motor turniketu. [9]

2.4 Přístupová práva

Nejdůležitějším řídícím faktorem přístupových systémů je přidělování **přístupového práva**, které se vystavuje konkrétním osobám na základě **stupňů oprávnění** podle prostorových, časových, personálních a jiných dispozic. U vyšších systémů se tak děje formou přidělení identifikačního média - nosiče, transponderu. [4]

Klasifikace stupně zabezpečení se pro každé přístupové místo normativně definuje pomocí třídy identifikace a třídy přístupu. K zabezpečení systému kontroly vstupů používáme **4 třídy identifikace (0 - 3)** a **2 třídy přístupu (A, B).** Klasifikaci zabezpečení můžeme definovat pro každé místo přístupu - odděleně pro vstup a pro výstup (biometrie při vstupu vs. odchodové tlačítko odchodu z objektu). **Klasifikace zabezpečení** je nezávislou kombinací tříd identifikace a tříd přístupu.

2.4.1 Třídy identifikace

Třída 0 - nevyžaduje přímou identifikaci a přístup je možný použitím jednoduchých tlačítek, kontaktů, detektorů pohybu atd. Při vstupu je nezbytná spoluúčast fyzické (vizuální) kontroly ostrahou. Vstupující osoba se prokazuje průkazem zaměstnance, občanským průkazem, návštěvnickou kartou, vstupenkou apod.

Třída 1 - vyžaduje znalost určité informace pro vstup. Touto informací je např. heslo, PIN kód. Instalované zařízení porovnává danou informaci s údajem v paměťové jednotce

a umožní vstup, pokud se shodují. „*Poměr počtu různých kombinací kódů k počtu identifikovatelných uživatelů musí být nejméně 1 000:1. Minimální počet kombinací v systému musí být 10 000.“* [5]

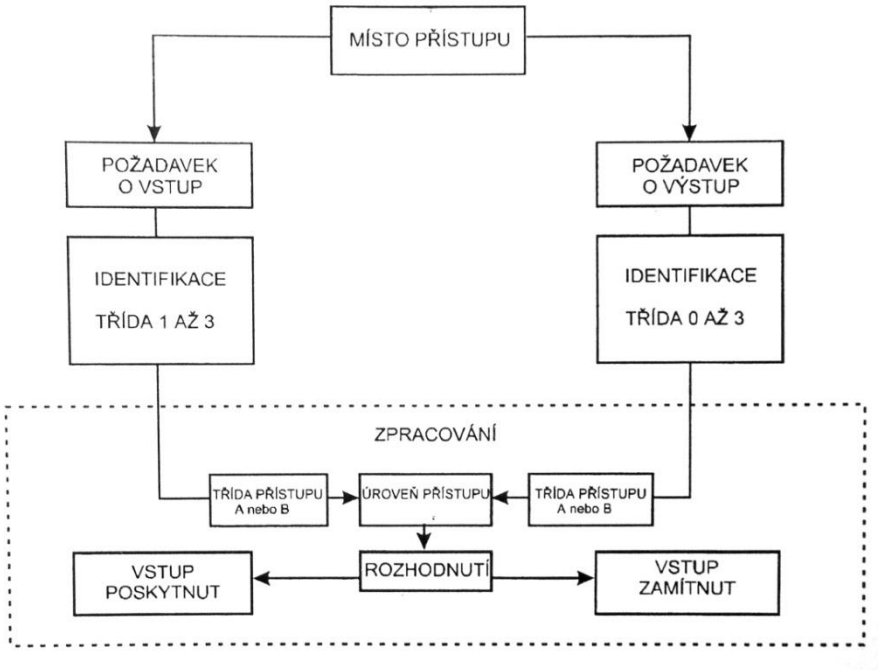
Třída 2 - vyžaduje použití pevného identifikačního prvku, jakým mohou být přístupové karty, čipové klíče anebo biometrické prvky vstupující osoby (otisk prstu, hlas, krevní řečiště). Každému uživateli musí být pro daný systém přiřazena jednoznačná identita. „*Struktura kódování identifikace musí poskytovat nejméně 1 000 000 kombinací a každá informace identifikace předaná do systému, musí být s touto strukturou porovnána. Četnost chybných povolení nesmí být větší než 0,01 %. Míra chybných odmítnutí musí být menší než 1 %. Identifikační prvek s kódovacími systémy, které jsou viditelné samotným lidským okem, a tudíž je možno při normálních podmínkách snadno zhotovit jeho duplikát, nesmí být použit. Pokud je identifikační prvek označen identifikačním číslem, nesmí být přímým zobrazením celého kódu identifikačního prvku.“* [5]

Třída 3 - využívá vzájemné kombinace prvků třídy 1 a třídy 2, jedná se tedy o kombinaci identifikačního prvku a biometrické metody. „*Informace uložené v paměti používané současně s identifikačním prvkem nebo biometrií musí mít minimálně 10 000 kombinací.“* [5]
Úroveň zabezpečení je samozřejmě ovlivněna řadou faktorů, ale nejdůležitějším z nich je počet kombinací a snadnost zhotovení duplikátu.

2.4.2 Třídy přístupu

Třída A - není vyžadován časový filtr, což znamená, že přístup není časově omezen. Také není vyžadováno ani ukládání informací o přístupu (registrace vstupů a výstupů).

Třída B - systémy musí používat časové filtry a musí ukládat informace o přístupech. Vyšší systémy ukládají do paměti další informace o otevření přístupu bez oprávnění včetně lokalizace daného místa, o napadení systému, otevření přístupu po uplynutí povolené doby, odmítnuté přístupy apod. Jako podtřídu můžeme uvést časový filtr bez ukládání dat.



Obr. 3 Tradiční postup povolení přístupu [3]

2.5 Identifikace a identifikační prvky

Subjekt může být jednoznačně identifikován těmito způsoby:

- tím, co subjekt zná, co si pamatuje - heslo, kód, kontrolní otázka,
- tím, co subjekt má fyzicky u sebe - identifikační karta, přívěšek, RF ovladač,
- tím, čím subjekt je - sám sebou, svými typickými rysy a chováním - biometrie.

Na základě výše uvedeného rozlišujeme:

1. **autentizaci heslem** - založené na znalosti hesla, které je utajené a známé jen uživateli; výhodou je jednoduchá technická realizace i cena; nevýhodou je relativně jednoduchá možnost odchycení hesla,
2. **autentizaci předmětem** - založeno na vlastnictví identifikačního předmětu; pro obecné označení autentizačního předmětu se užívá termín token; výhodou je vyšší úroveň zabezpečení; nevýhodou je možnost odcizení autentizačního předmětu,
3. **biometrickou autentizaci** - založeno na biometrických charakteristikách osoby; výhodou je vysoká míra zabezpečení; nevýhodou vysoká cena zařízení.

Typů identifikační prvků je nepřeberné množství. Můžeme je dělit například z hlediska styku prvku se snímacím zařízením na kontaktní a bezkontaktní, popřípadě podle principu jejich činnosti nebo tvaru.

Rozdělení identifikačních prvků:

Manuální – řadíme sem vypínače, kódové zámky. Jsou pasivní, vyžadují manuální vstup od člověka.

Čipové - identifikátor je uložen v integrovaném obvodu (čipu, paměti), možnost čtení i zápisu.

- kontaktní - kontaktní čipové karty (SmartCard), iButton čipy,
- bezkontaktní - bezkontaktní čipové karty/přívěšky, RFID,
- kombinovaná - kombinace kontaktní i bezkontaktní v jedné kartě, přívěsku, klíči.

Magnetické - karty s magnetickým proužkem, průtažné čtečky.

Optické - čárový kód, data matrix (2D) nebo kruhový kód. Laserové nebo CCD čtečky.

Radiofrekvenční - např. bluetooth identifikace, využití bezlicenčních pásem 434/868 MHz/2,4 GHz.

Biometrické - papilární linie, oční duhovka, 3D model hlavy, DNA apod. [9]

Obr. 4 Ukázka čipů iButton

2.6 Druhy přístupových systémů

2.6.1 Klasické zabezpečovací prostředky

Možností zamezení přístupu u klasických druhů ohraničujících prostředků přístupových systémů jsou:

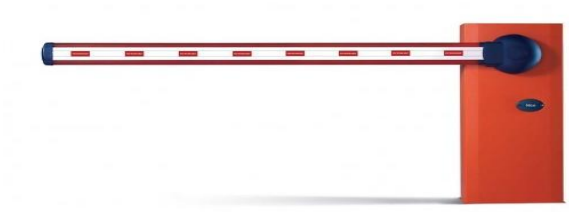
- vstupní dveře a vrata; okna a mříže,
- brány - turnikety, závory,
- rámové průchozí detektory.

Vstupní dveře - musí být vyrobeny z tuhé konstrukce, která je pevně ukotvena do zdí. Ovládány bývají manuálně nebo motoricky. Tyto prvky obvodové ochrany mají zamezit vstupu osob bez patřičného povolení. Zpravidla u nich bývá zabudovaný docházkový systém.

Turniket - používá se při kontrole vstupu osob v místech velkého provozu jako např. u velkých podniků, sportovních areálů a podobně. Turnikety se používají pro mechanickou blokaci vstupu (při nezaplaceném jízdném, u vstupů do podniku pro selekci jednotlivců a možnosti jejich vizuální kontroly). Bezpečnostní účinek turniketů není na vysoké úrovni a řadíme je mezi nejméně bezpečné vstupní zařízení. Nepovolaná osoba může snadno projít, pokud není turniket vybaven další mřížovou konstrukcí. Samotná konstrukce tohoto zařízení většinou umožní nežádoucí přístup i více osobám najednou, a proto je vhodný pro objekty s nízkou požadovanou úrovní zabezpečení nebo jako doplňkové zařízení pro místa např. s fyzickou ostrahou.

Obr. 5 Turnikety (SAITECH TW-AP 1100, WHD 04, ERA 90) [20]

Závora – jedná se o vstupní zařízení, které je vhodné pro omezení vjezdu automobilů do objektu nebo daného prostoru. Zavřená závora znemožňuje volný vjezd či průjezd aut, ale její konstrukce umožňuje průchod osob. Závora má pouze kontrolní funkci a nemůže nijak zabránit násilnému vniknutí. Vhodné využití pro toto zařízení jsou parkoviště. Závory mohou být poháněny elektromotoricky nebo manuálně tak, že ostraha po zkontrolování vozidla závoru zvedne.



Obr. 6 Závora WIL 4 KCE [22]

Dveře s elektromagnetickým zámkem - nejbezpečnější vstupní zařízení z dosud uvedených. Obecným předpokladem je, že neautorizovaná osoba není schopna otevřít dveře bez použití hrubé síly. U dveří je umístěn terminál, který odemkne dveře po úspěšné identifikaci a autorizaci. Po otevření dveří je však umožněn průchod i více osobám.

V případě důležitých institucí přistupuje k problematice ochrany vstupů i ochrana proti teroristickým živlům. Znamená to, že přístupové systémy musí řešit i otázku odhalení zbraní, kovových předmětů a výbušnin u sledovaného vstupu. Tuto otázku řeší různé typy turniketů - **detekčních rámů**, které využívají princip magnetického pole, ultrazvuku a rentgenových paprsků. [5]

2.6.2 Mechanické zabezpečovací prostředky

Jde o mechanické prvky a systémy, které jsou většinou přímou součástí přístupových systémů a zařízení. Řadíme sem především:

- dveřní zámek (zadlabací, rozvorový, vrchní),
- elektromechanická cylindrická vložka,
- zámky elektromotorické,
- zámky s čipovým klíčem.

2.7 Způsoby přístupu

Pro způsoby přístupu se jako vstupní média využívají především následující akční prvky a systémy:

1. klávesnicový systém,
2. kartový systém,
3. čipový vstup (iBUTTON),
4. systém Hands free,
5. vstupová a signalizační čidla,
6. kamerové systémy včetně videotelefonu,
7. biometrické systémy.

Klávesnicové systémy umožňují přístup po zadání stanoveného kódu nebo hesla. Při zadání správného hesla elektronika odblokuje přístupovou zábranu, kterou může být dveřní zámek, závora apod. [13]

Kartové systémy dělíme:

1. Podle funkčního média:
   - s magnetickým kódem,
   - s čárovým kódem klasickým (EAN8, EAN13, CODE 3 of 9),
   - s čárovým kódem dvojrozměrným (PDF 417),
   - s mikročipovým kódem (postupně 4 bitový, 8bitový, 16 a 32bitový).

2. Podle způsobu používání:
   - kontaktní (induktivní, optické),
   - bezkontaktní.

V systému hands free se používají čipové bezkontaktní karty s dosahem 1 až 5 metrů, přičemž karta může být ponechána v kapse saka nebo připevněna za oknem automobilu. [5]

V současnosti jsou kartové systémy hojně používány a mají širokou platformu výroby a využití. Důležitým prvkem je nosič transponderu (mikročipu), který se objevuje nejčastěji ve formě plastové karty.

Rozlišujeme tyto typy:

A - karty platební,

T - karty telefonní,

Z - karty kontroly přístupu.

Rozměry karet jsou celosvětově standardizovány na rozměr 54 x 85,5 mm a tloušťku 0,8 mm.

Biometrické systémy

Širokou oblastí autentizačních metod jsou biometrické autentizační přístupy, které využívají k ověření identity osob biometrických parametrů. Řadí se mezi nejmladší identifikační systémy.

Biometrická identifikace vychází z předpokladu, že některé fyziologické (anatomické) charakteristiky člověka jsou jedinečné a časem neměnné. Jejich činnost je založena na porovnávání údajů biologických vlastností jednotlivců. Základním předpokladem je dostatečná kapacita počítačů nutná pro zpracování podstatných identifikačních informací vložených do paměti počítače. Pak už následuje pouze porovnání biometrických údajů získaných čtečkou s údaji uloženými v počítači. Výsledek porovnání záleží na množství a kvalitě informací zadaných do počítače.

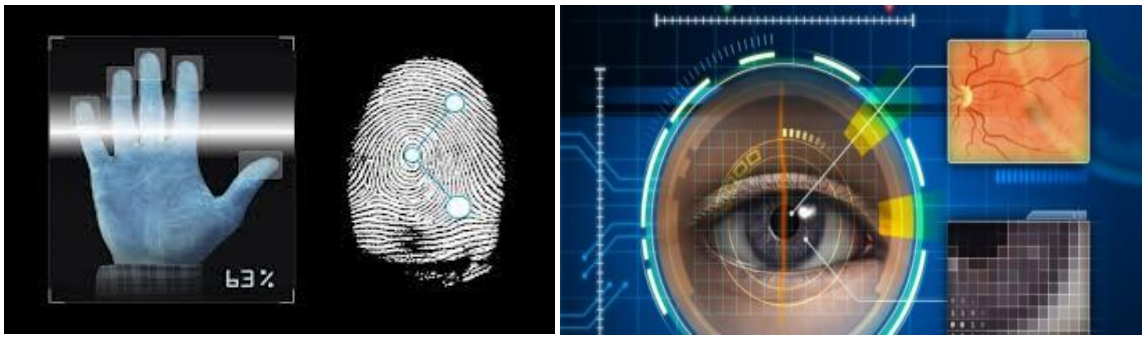
Systémy, které využívají biometrické ověření nepotřebují žádné věcné pomůcky (klíče, identifikační karty), což představuje výhodu, protože přenos identifikačních znaků u ostatních používaných metod je tím nejzranitelnějším místem. Na druhé straně potřebují ale podstatně složitější snímací zařízení. Objemy porovnávaných dat s databází jsou velmi vysoké, což zpomaluje odezvu celého systému, proto se v praxi dosti často používá kombinací s další vhodnou metodou (např. identifikace kartou), a to z důvodu rychlejší odezvy systému. [14]

Snímače biometrických rysů se instalují zejména tam, kde je třeba nejvyššího stupně ochrany v režimové oblasti.

Mezi nejpoužívanější biologické prostředky řadíme:

- **Otisk prstů a dlaně** - využívají poznatek, že na světě nejsou dvě osoby, které by měly stejné papilámí linie na prstech či dlani. Zařízení vyžaduje přímý fyzický kontakt,

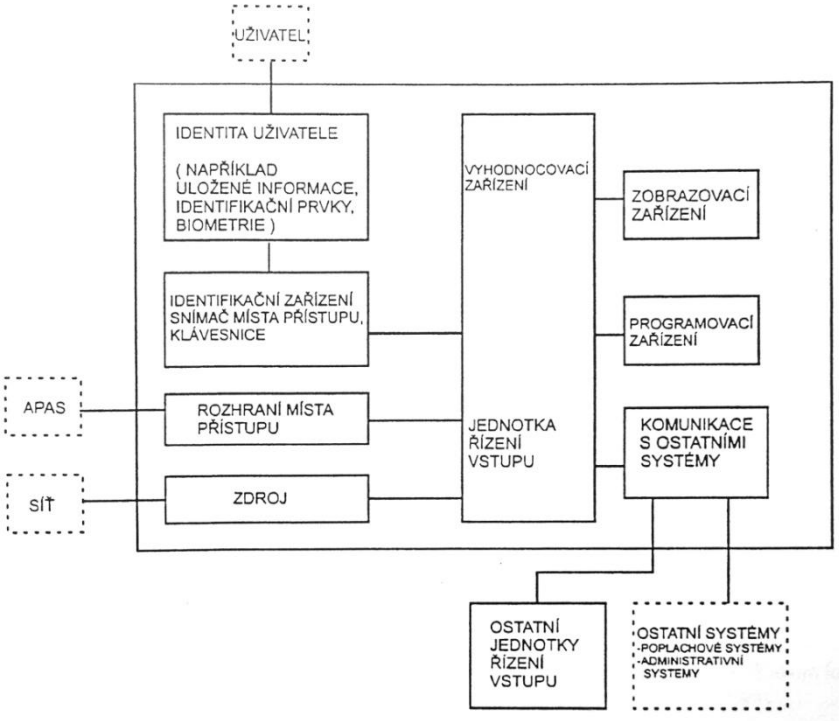
- **Hlas** - hlasová identifikace rozezná i napodobený hlas, ale není tak bezpečná při snímání, existuje možnost dokonalého záznamu i reprodukce hlasu nositele a počítačová syntéza řeči,
- **Obraz oční duhovky** - identifikační kontrola je bezkontaktní metodou vyžadující pouze přesné postavení hlavy a optimální osvětlení oka,
- **Obraz obličeje** - identifikace obličeje je rovněž bezkontaktní metodou, která využívá snímání hlavy, resp. obličeje pomocí speciální kamery. Při snímání se využívá infračervené (IR) světlo, tím pádem je vyloučeno použití fotografie či obličejové masky, [5]
- **Oční sítnice** - optický systém sejme část sítnice, obraz tvoří krevní cévky. Uživatelsky nepřívětivé, nutná velmi přesná pozice vůči skeneru,
- **Tvar ruky, ušnice, pach, rozložení cév, DNA.** [9]



Obr. 7 Biometrická identifikace dlaně a oka [17]

2.8 Zavedení přístupového systému

Přístupové systémy se instalují podle stupně důležitosti zabezpečení. *Konkrétní řešení přístupu se posuzuje podle mnoha faktorů, z kterých jsou bezpečnostní rizika, ať už hmotná, fyzická nebo informačního charakteru, tím nejdůležitějším.* [9] Bezpečnostní oblasti strategických podniků, státních institucí, výpočetních center, bank, trezorů atd., mají přístupové systémy důmyslnější a mnohdy s několikanásobnou kontrolou a zajištěním. U ostatních realizací jako je například střežení obchodních nebo činžovních domů, provozoven apod., se instalují systémy méně náročné, ale přesto naprosto bezpečné pro daný druh ochrany.



Obr. 8 Blokové schéma přístupového systému [3]

Při zřizování systému kontroly vstupů je velmi důležité zvolit optimální systém z hlediska použití, nutné bezpečnosti a účinné kontroly vstupu. *„Nejčastějším vstupním opatřením je fyzická kontrola ostrahou mnohdy doplněná jednoduchými kontrolními či signalizačními prostředky. Systémy kontroly vstupů jsou podstatnou částí celkové ochrany objektu a jsou většinou napojeny na systémy elektronické ochrany. Při jejich realizaci je nutné mít na zřeteli plnění jejich bezpečnostních požadavků a funkčních vlastností, které jsou stanoveny v normě ČSN EN 50133-1. Pokyny pro aplikace jsou uvedeny v normě ČSN EN 50133-7.“* [5]

V uvedené normě jsou stanovena doporučení pro:

- postup a rozbor kritérií a vlivů, které je třeba akceptovat při návrhu systému,
- požadavky na provádění jednotlivých etap výstavby systému,
- požadavky na zajišťování revizí,
- způsob provádění kolaudace a předávání systému,
- požadavky na způsob kontrol a provozování systémů,
- požadavky na údržbu celého systému,
- rozsah projektové a provozní dokumentace.

Požadavky na konstrukční prvky jako jsou závory, turnikety a podobné, uvádí předpisové normy zpracovávané technickou komisí CEN/TC 33. Stejně tak je pro řešení dané problematiky podstatná i vyhláška Národního bezpečnostního úřadu o objektové bezpečnosti č. 339/99 Sb., Elektrická zámková zařízení a systémy pro zabezpečení oblastí, zařízení a systémy sloužící k elektronickému prokazování oprávněnosti a totožnosti osob. [5]

2.9 Architektura sítě

Rozsáhlejší SKV systémy jsou prostřednictvím hlavní řídicí jednotky spojeny s aplikačním a databázovým serverem, a to nejčastěji prostřednictvím 3vrstvé architektury s tímto uspořádáním:

1. **vrstva** představuje uživatelské prostředí (terminály, čtečky, hardware SKV),
2. **vrstva** představuje vlastní aplikace/program (aplikační server),
3. **vrstva** představuje databázi uživatelů a přístupových práv (SQL server). [9]

Jednovrstvá architektura soustředí veškerou inteligenci do jednoho centrálního počítače, u dvojvrstvé architektury existuje databázový server a klient, a výkon je soustředěn na straně serveru nebo na straně klienta. Třívrstvá architektura je vhodná pro dosažení optimálního výkonu a stability systému. [10]

2.10 Integrace s jinými systémy

Přístupové systémy mohou být provázány s jinými slaboproudými systémy. V praxi existují převážně kombinace s těmito systémy:

- **Poplachový zabezpečovací a tísňový systém (PZTS)** - sofistikovanější sběrnicové systémy PZTS často podporují základní funkce přístupových systémů, výhodou je zde možnost ovládat systém prostřednictvím přístupových identifikátorů, monitorovat stav PZTS za dveřmi na čtečce apod. (otevření dveří a zároveň odjištění PZTS).
- **Elektrická požární signalizace (EPS)** - je vždy samostatná, při evakuaci nebo požáru je však nutné zajistit správnou funkci všech přístupových bodů - odblokovat únikové cesty, zablokovat požární prostupy apod.

- **Kamerový systém (CCTV)** - systém může při časové synchronizaci poskytnout doplňkové obrazové informace ke každé prostupové události.
- **IT systémy** - samostatnými čtečkami identifikačních médií, připojenými k PC, se může řídit přístup k PC, k síti apod.
- **Měření a regulace** - přítomnost osob může např. automaticky přizpůsobit vytápění, osvětlení, výtahy apod.

Můžeme se však setkat s tím, že některé prameny do těchto systémů zahrnují i docházkový a stravovací systém (viz kolektiv autorů T. Vítek, M. Husák, T. Teplý [9]. Přičemž v **Docházkovém systému** jsou použity jak docházkové tak i přístupové funkce. Naopak **Stravovací systém** využívá především shodných identifikačních médií, ale jinak jde o samostatný systém. [9]

3 DOCHÁZKOVÉ SYSTÉMY

3.1 Vymezení pojmu

Docházkové systémy provádí kontrolu oprávnění vstupu na konkrétním místě vstupu a mohou následně provozovat sběr informací o čase a důvodech průchodu daným místem vstupu např. s návazností na mzdovou agendu. [5]

Docházkové systémy jsou využívány společnostmi všech velikostí pro záznam pracovní doby svých zaměstnanců. Výstupy těchto systémů lze použít pro efektivní řízení, ale hlavním důvodem je přesný podklad pro výpočet mzdy zaměstnanců. Docházkový systém umožňuje zaměstnavateli poskytnout plnou kontrolu všech zaměstnanců. Odpadá nutnost ručního přepočítávání údajů z papírové karty zaměstnance, protože tato důležitá elektronická data jsou zpravidla poskytována na účetní a personální oddělení. DS chrání společnost před podvody s odpracovanými hodinami a šetří mzdové náklady úsporou pracovních sil při zpracování mzdových podkladů.

Ucelený systém pro evidenci a zpracování docházky svou koncepcí nabízí spolehlivé řešení a vysoký komfort pro uživatele. Samozřejmostí je vedení agendy podle požadavků Zákoníku práce, zákon č. 262/2006 Sb., která ukládá zaměstnavateli povinnost evidovat docházku svých zaměstnanců.

3.2 Výhody docházkových systémů

Docházkový systém umožňuje rychlou registraci osob na elektronických terminálech pomocí osobních bezkontaktních identifikátorů (klíčenky, příp. karty) nebo pomocí biometrických prvků (otisk prstů, dlaně, oční duhovka, hlas). Zejména u velkých firem s velkým počtem zaměstnanců je rychlý vstup na pracoviště významnou devizou. Jestliže firma disponuje více vchody v rámci jednoho objektu, je přínosné nainstalovat docházkový systém ke každému jednotlivému vchodu.

Vedoucím pracovníkům znatelně zjednodušuje administrativní práci spojenou s evidencí a kontrolou docházky svých podřízených pracovníků. Systém ukazuje aktuální přítomnost pracovníka na pracovišti i celkový čas, který zde strávil. Dále lze snadno kontrolovat například pozdní příchody, přetažení poledních přestávek v práci nebo vstupy do budovy mimo pracovní dobu. U areálů, které podléhají přísnějším bezpečnostním podmínkám, lze monitorovat pohyb osob a řídit přístup do jednotlivých objektů.

Přístupový i docházkový systém se v praxi často propojuje a vytváří tak **integrovaný identifikační systém kontroly vstupu.**

Obr. 9 Čtecí zařízení pro řízení přístupu do budovy

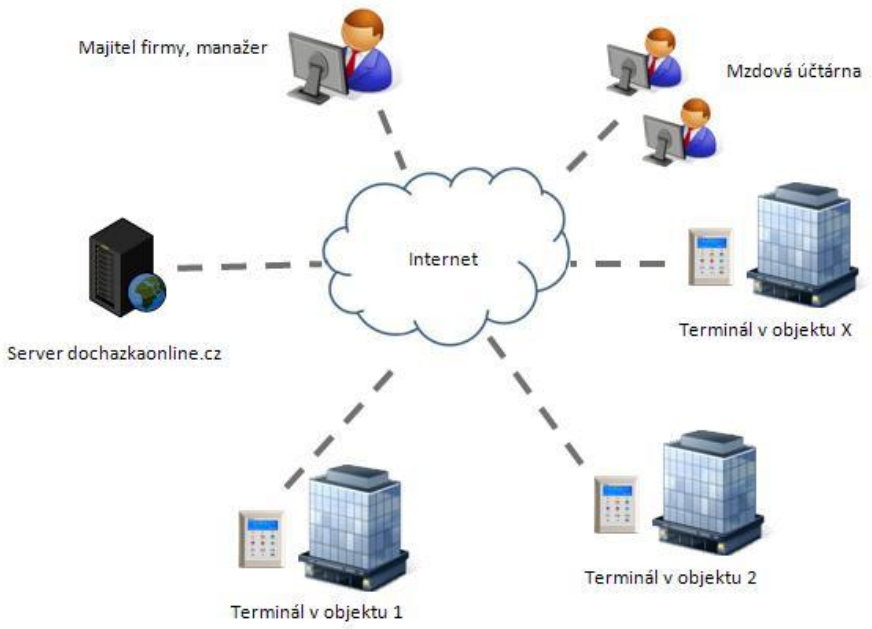
Podstatou systému kontroly vstupu je zabránění přístupu neoprávněných osob do vyhrazených prostor, nebo zabránění přístupu k důležitým či utajovaným informacím. Systém umožňuje sledování pohybu osob v definovaných zónách, jejich vyhledávání, kontrolu jednotlivých průchodů atd., což je prováděno technickými prostředky od jednoduchého snímače identifikační karty bez evidence až po ucelený on-line systém s centrální evidencí, analýzou a eventuelním napojením na další aplikace. [5]

Obr. 10 Vstup do budovy opatřené terminálem, identifikace osoby [15]

V současné době existuje už jen malé množství společností, které stále používají papírové karty pro evidenci docházky svých zaměstnanců. Jedná se zejména o firmy s malým množstvím zaměstnanců a implementace docházkového systému by pro ně neměla ten správný efekt.

3.3 Funkční požadavky na docházkový systém

- správa oprávnění uživatelů ke vstupu do chráněných zón podle přístupových práv,
- registrace nového pracovníka, včetně editace jeho osobních dat,
- správu budov, místností a příslušných vstupních zařízení,
- kontrolovat pohyb osob po areálu podle časového období, objektu,
- omezení přístup do jednotlivých částí aplikace podle rolí.



Obr. 11 Schéma docházkového systému [16]

3.4 Docházkové terminály

Pro účely identifikace osob lze využívat několik typů docházkových terminálů a snímačů. Volba konkrétního typu terminálu závisí na požadavcích samotného investora. Kvalitní dodavatel je schopen poradit a umí dodat řešení šité na míru potřebám konkrétního podniku. Zařízení může zároveň sloužit pro otevírání vstupních dveří nebo také pro

odblokování turniketů. Terminály dělíme podle mnoha kritérií, zejména podle konstrukčního provedení, způsobu komunikace a způsobu identifikace osoby. Volba terminálu má zásadní vliv na funkci požadovaného řešení. Mezi další možnosti pro volbu terminálů patří - identifikace osob bezkontaktní kartou nebo otiskem prstu, zabezpečení proti duplikátům karet, připojení do sítě přes ethernet, sériovou linkou (RS-232, RS-485), případně wi-fi, ovládání přes klávesnici nebo dotykový displej, zobrazení informací o odpracované době ihned na displeji, provoz on-line i off-line a záloha proti výpadku elektrické energie.

Obr. 12 Ukázky panelů docházkových terminálů

3.5 Software docházkového systému

Software pro evidenci docházky poskytuje uživatelům zobrazení dat v několika úrovních. Docházkový software je síťový a mohou jej využívat jak vedoucí pracovníci, tak i jednotliví zaměstnanci v závislosti na přidělených přístupových právech. V rámci vyhodnocení může uživatel s přístupovým právem vedoucího provádět ruční opravy dat včetně doplnění chybějících záznamů. Pro internetové uživatele bývá také k dispozici webová nadstavba.

Jak v České republice, tak i v zahraničí existuje celá řada společností, které dodávají systémy k evidenci docházky. Tyto firmy se většinou zabývají nejen vývojem docházkových systémů, ale všeobecně vývojem systémů, které ke své činnosti využívají přístupové terminály nebo senzory pohybu.

Z velké škály dodavatelů si můžeme vybrat např. mezi těmito: Advent spol. s r.o., JABLOTRON, a.s., EVVA Sicherheitstechnologie GmbH, ANeT-Advanced Network

Technology, s.r.o., IReSoft, s.r.o., TEchnodat – CAE – systémy, s.r.o., ASSA ABLOY Czech & Slovakia s. r. o., PHOBOS, s.r.o., SLIM, s.r.o., IVAR, a.s.

3.6 Zavedení docházkového systému

Důvodů pro zavedení docházkových systémů je celá řada, mezi ty nejpodstatnější můžeme zařadit tyto:

- automatická kontrola příchodů do zaměstnání (pozdní příchody),
- možnost sledování pohybu osob po areálu,
- pohyb osob v budově je možno omezit v čase,
- možnost měnit přístupová oprávnění z jednoho místa,
- automatizované získání statistických informací pro řízení firmy,
- možnost zpoplatnění pobytu osob v určitých prostorech (např. parkoviště, fitcentra, bazény).

II. PRAKTICKÁ ČÁST

4 POPIS OBJEKTU

Popisovaný objekt administrativní budovy je situován v samotném centru města. Jedná se o renesančně a barokně přestavěnou pozdně gotickou budovu představující společenskou i architektonickou dominantu města. Zcela určitě se dá říct, že jde o symbol staleté městské samosprávy.

Původně šlechtický dům prodal městu na stavbu radnice v roce 1702 hrabě Dominik Ondřej z Kounic. Pod přední částí budovy se nacházejí rozsáhlé podzemní prostory jako součást sítě chodeb pod středem starého města. Závažná slohová přestavba (nástavba věže, interiérové úpravy, přefasádování) byla provedena v baroku v letech 1703 – 1715. Z této doby je dochován půdorys radnice do dnešních dnů.

Jako zajímavost se často zmiňují věžní hodiny, které zhotovil hodinář František Lang a v roce 1723 je doplnil soškou Černého Janka, k němuž se váže známá pověst z doby kuruckých válek.

Obr. 13 Kresba radnice
[interní dokumentace]

Protože se jedná o budovu místní samosprávy malého města veřejnosti volně přístupnou, není zde zavedena fyzická ostraha bezpečnostní firmou ani vlastním strážným. Budova celkově disponuje třemi nadzemními podlažími a jedním podzemním podlažím.

Do budovy je možné vejít přes dva vstupy. Hlavní vstup přes mohutné dvoukřídlé dřevěné dveře přímo z náměstí a boční vstup z postranní ulice.

4.1 Popis jednotlivých podlaží

4.1.1 Podzemní podlaží

Vstup do podzemního podlaží je situován ve vstupní hale u bočního vchodu do budovy. Podzemí je z jedné strany vstupu chráněno uzamykatelnou mříží a z druhé strany je vstup možný pouze přes kancelář, která není veřejnosti přístupná. Prostup celým podzemím je chráněn uzamčenými dveřmi. Nachází se zde zrekonstruované historické sklepení a rozsáhlý archiv. Podzemí není zcela odkryto a nachází se zde také chodba, která je zavalena a dá se tušit, že v dřívějších dobách to byla úniková cesta z této budovy do některých z domů ležících na náměstí. Na zabezpečení těchto prostor bych nic neměnila, shledávám je naprosto dostačující a z tohoto důvodu bych jej ponechala v současném stavu.

4.1.2 První nadzemní podlaží

První nadzemní podlaží obsahuje samozřejmě oba vstupy do budovy a pracoviště, kde je velký pohyb občanů. Je zde podatelna, matrika, evidence obyvatel a několik pracovišť pro agendu občanských průkazů a cestovních pasů. Dále se zde nachází velká zasedací místnost s příslušenstvím, další archiv, dva příruční sklady a pracoviště údržby. Boční vstup do budovy je bezbariérový a vzhledem k tomu, že se v jeho blízkosti na nádvoří nachází rovněž výtah, mohou úřad bez potíží navštěvovat handicapovaní občané či maminky s dětmi v kočárcích.

4.1.3 Druhé nadzemní podlaží

Do druhého nadzemního podlaží se můžeme dostat dvěma schodišti nebo výtahem. V tomto podlaží se nachází sekretariát a kanceláře vedení města, tzn. kancelář tajemníka, starosty a obou místostarostů. K těmto prostorám přiléhá další zasedací místnost. Dále je zde finanční odbor, oddělení informatiky, pracoviště interního auditu a tiskové mluvčí.

4.1.4 Třetí nadzemní podlaží

Poslední, tedy třetí nadzemní podlaží, je přístupné přes centrální schodiště a samozřejmě také výtahem. Nachází se zde kanceláře správy majetku města, právního oddělení, odboru

rozvoje města, oddělení dotací a rozvoje města a v neposlední řadě také pracoviště zvláštních úkolů a krizového řízení. Najdeme zde také malé příruční sklady, které jsou situovány téměř po celé délce chodby pod střešními okny. Dále velký archiv a kotelna. Z posledního podlaží je samozřejmě možné vystoupat na radniční věž.

Naprostá většina místností a chodeb není chráněna detektory pohybu. Jištění kanceláří je pouze přes klasické dveřní zámky. Elektronický zabezpečovací systém se nachází v prostorách se servery, v prostorách pro zvláštní úkoly a krizové řízení, dále na pracovišti občanských průkazů a cestovních dokladů a jištěna jsou historické hodiny a obrazy, které jsou umístěny v zasedací místnosti 2. nadzemního podlaží.

Celkově je možno konstatovat, že budova je v dobrém technickém stavu. Vzhledem ke stáří objektu a zejména k historické hodnotě je nutné pravidelně provádět opravy a údržbu pod dohledem pracovníků státní památkové péče. Poslední velká investice proběhla v roce 2012 při opravě celého pláště budovy, která tak má novou fasádu z vnější i vnitřní strany a opravy se dočkala také radniční věž. V rámci těchto oprav došlo i k náročnému restaurování sošky Černého Janka, která má své nezastupitelné místo na této věži a svým zvoněním krátce před každou celou hodinou dává celému městu vzpomenout na dobu, kdy tímto svým zvoněním zachránil město před vpádem a vypleněním nepřáteli.

Obr. 14 Letecký snímek budovy [19]

4.2 Popis stávajícího systému ochrany

4.2.1 Perimetrická ochrana

Perimetrická (obvodová) ochrana zde není řešena, protože budova se nachází v centru města. Ze dvou stran, severní a západní, vede kolem budovy chodník a silnice. Z těchto stran je také budova osvícena veřejným osvětlením. Východní strana přiléhá k sousední budově, jižní strana s nádvořím a vysokou cihlovou zdí sousedí částečně se sousední budovou a částečně s jejich zahradou. Objekt je přístupný přes vchody ze dvou světových stran. V úvahu musíme vzít i skutečnost, že možný narušitel by do areálu objektu mohl vniknout
i překonáním zídky ze sousedního pozemku.

4.2.2 Plášťová ochrana

Budova je opatřena pouze vnějším kamerovým systémem, který je umístěn na věži budovy a je situován směrem na náměstí. Účelem této kamery je sledovat dění zejména na náměstí a u hlavního vchodu do budovy.

4.2.3 Prostorová ochrana

Na obou vstupech je instalovaný systém ACS. Hlavním úkolem ACS je umožnění vstupu do administrativní budovy nejen oprávněným osobám (zaměstnancům), ale také návštěvám a hlavně široké veřejnosti-občanům v určitém režimu vstupu. Vstup je umožněn v uživatelsky nastavitelné době a v rozsahu oprávnění stanovené z bezpečnostních hledisek správcem systému. ACS je integrovaný s docházkovým systémem.

PZTS je, jak jsem již stručně uváděla, instalovaný pouze na vybrané kanceláře, a to na kanceláře evidence, zpracovávání a uchovávání občanských průkazů a cestovních dokladů, pracoviště zvláštních úkolů a krizového řízení a dále na místnost s centrálním počítačem, tzv. servrovnu. Vnitřní kamerový systém není instalován.

4.2.4 Předmětová ochrana

Signalizuje napadení nebo neoprávněnou manipulaci s chráněnými předměty. V našem případě se konkrétně jedná o cenné obrazy a historické sloupové kyvadlové hodiny. Poplach je vyhlášen na základě bezprostřední přítomnosti pachatele u chráněného předmětu nebo na základě manipulace s tímto předmětem.

Jak jsem uváděla, na poplachovou aplikaci jsou připojeny sloupové astronomické hodiny a hodnotné obrazy, které se nacházejí v prostoru radnice v druhém nadzemním podlaží. Pro lepší představu o hodnotě a tedy důvodu zabezpečení krátce nastíním popis těchto předmětů.

Astronomické hodiny Vilibalda Růžičky

Vilibald Růžička byl učitel, ředitel, odborný pracovník muzea, spisovatel a vlastenec. Prosazoval všestranný pokrok a vrcholem jeho technické činnosti je orloj, který je umístěn právě zde na radnici. Růžičkovy astronomické hodiny představují unikátní astronomický orloj obohacený o velké množství časoměrných funkcí. Srdcem mechanismu je přesný hodinový stroj se sekundovým kyvem. Kromě hlavního ciferníku obsahuje další čtyři samostatné ciferníky ukazující sekundy, měsíce, dny a data. Astronomická část se skládá z astronomické sféry, otočné hvězdné mapy, globusu a z ciferníků. Na tomto orloji se astronomická část a kalendářní část prolínají. Stroj řídí pohyb ručně zhotovené mapy hvězdné oblohy, která znázorňuje momentální polohu hvězd nad nočním obzorem. Mapa se otočí jednou za hvězdný den, ten je měřen hvězdným časem, předbíhající občanský zhruba o čtyři minuty za 24 hodin. Z tohoto důvodu také každý týden v určený den dochází pracovník místní hvězdárny, aby hodiny seřídil a natáhl kyvadla. Jako další zajímavost uvedu, že hodiny trvale ukazují středoevropský čas, protože všechny ostatní údaje jsou od tohoto času odvozeny.

Obr. 15 Astronomické hodiny

Hodiny jsou v budově veřejnosti přístupné ve 2. nadzemním podlaží, ale vzhledem k jejich unikátnosti jsou připojeny k poplachovému a zabezpečovacímu systému. Zabezpečení hodin je zajištěno pomocí **otřesového detektoru**. Otřesový detektor je vybaven velmi citlivým senzorem, který zachytí i malé otřesy nebo vibrace. Výstupní kontakt předá tuto informaci do ústředny PZTS a ten vyvolá poplach. Některé otřesové detektory jsou vybaveny regulací na nastavení citlivosti detekce otřesu. Otřesová čidla se využívají převážně pro ochranu věcí.

Historické obrazy

Jedná se o několik obrazů větších formátů, které zobrazují život a zvyklosti v daném regionu Moravského Slovácka, konkrétně města samotného a také přilehlých míst. Obrazy nemůže veřejnost běžně shlédnout, protože jsou umístěny ve druhém nadzemním podlaží v zasedací místnosti, která není volně přístupná. Obrazy jsou zajištěny **magnetickými kontakty**. Funkce magnetického kontaktu je založena na principu jazýčkového relé spínaného magnetickým polem permanentního magnetu. Pro instalaci je možné použít magnetické kontakty pro povrchovou nebo zápustnou montáž vodičů.

Obr. 16 Ukázka zabezpečených obrazů

4.3 Popis docházkového systému

Vzhledem k tomu, že v rámci daného přístupového systému je každý zaměstnanec jednoznačně identifikován, jsou jeho osobní data provázána s dalšími funkcemi systému, a to zejména s docházkovým systémem. Současnou funkcí přístupového systému je kontrola docházky zaměstnanců. Systém je na všech vstupech, resp. výstupech vybaven dotykovým docházkovým terminálem.

Při přiložení čipu na čtečku docházkového terminálu při vstupu do budovy je automaticky zahájena pracovní doba zaměstnance. Použije přesný čas, to znamená, že systém pracuje i s minutami. Stejně tak při odchodu a přiložení čipu je pracovní doba ukončena. Na terminálu je také možné přiložením čipu zadat důvod přerušení pracovní doby. O zaznamenání údaje na docházkovém terminálu je pracovník upozorněn většinou krátkým zvukovým signálem. Na počítači v prostředí dodaného softwaru si pak může každý zaměstnanec prohlédnout svůj pracovní výkaz. Vedoucí pracovníci mají možnost na základě přiděleného oprávnění nahlížet do pracovních výkazů svých podřízených a také provádět editaci v jejich výkazech. Aplikace, která nyní zajišťuje provoz docházkového systému, se jmenuje PowerKey a je od společnosti Advent.

Obr. 17 Panel docházkového terminálu

Na docházkovém terminálu můžeme jednoduše zaznamenat požadovanou úlohu zápisu podle piktogramů či kombinací piktogramů a popisu, které jsou umístěny u každé čtečky čipů. Popis jednotlivých funkcí docházkového terminálu je uveden dále.

4.3.1 Funkce docházkového terminálu

Jednotlivé funkce docházkového terminálu, který je umístěn v budově:

Příchod – zaznamená přesný příchod do objektu

Oběd – zaznamená odchod na zákonem stanovenou přestávku v práci – oběd. Délka trvání oběda je stanovena na 30 minut. Při pozdějším návratu se tento čas navyšuje

o každou další minutu. V případě dřívějšího návratu z této přestávky je sice tento čas zaznamenán, ale do mzdových podkladů je přenesen jako přesných 30 minut.

Lékař – zaznamená odchod k lékaři

Paragraf – zaznamená odchod k ošetřování člena rodiny

Služebně – zaznamená odchod či odjezd na služební cestu

Dovolená – zaznamená odchod na dovolenou

Odchod – zaznamená čas odchodu z objektu

Saldo – ukáže aktuální saldo pracovníka

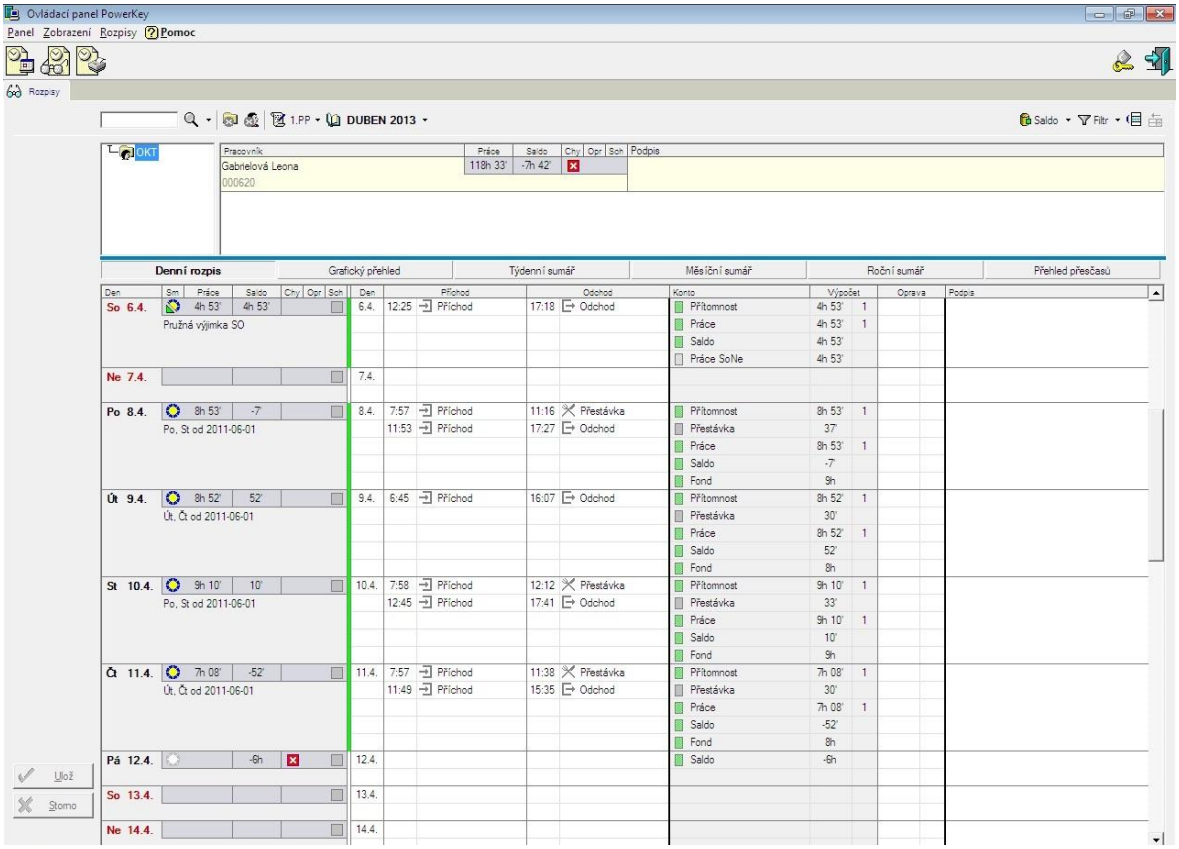
Docházkový systém je systém, jehož základní funkcí je evidování docházky zaměstnanců a sběr relevantních informací pro mzdovou účtárnu.

Uživateli, resp. zaměstnanci z držení docházkového čipu vyplývají zejména tyto povinnosti:

- jednoznačná odpovědnost uživatelů,
- každý uživatel má jasně stanovené pravomoce přístupu nadefinované v přístupovém čipu,
- pravomoce jsou vázané na funkce pozice zaměstnance a jeho pracovní zařazení,
- povinnost zaměstnance zabránit možnému zneužití čipu neoprávněnou osobou,
- zodpovědnost za svěřený majetek (podpis o převzetí přístupového čipu).

4.3.2 Výhody a přínosy implementace DS

- identifikace zaměstnance na docházkových terminálech,
- on-line přehled o aktuálním stavu odpracované doby, sledování různých období,
- schvalování docházky a plánovaných absencí vedoucími pracovníky,
- plánování nepřítomnosti na vybraná období, možnost propojení na webový portál,
- tvorba přehledových sestav (bonusy, stravenky),
- propojení do programu pro zpracování mezd, tisk pracovních výkazů,
- nastavení přesměrování telefonů na pracovníka, který je přítomen (při rozšíření systému).



Obr. 18 Ovládací panel docházkového systému PowerKey

Uvedený obrázek představuje rozhraní, které si může prohlédnout každý zaměstnanec, resp. každý zaměstnanec se může přihlásit pouze ke svým údajům. Může si zde nastavit zobrazení, ale nemá možnost jakkoliv upravovat uvedené údaje. Pravomoci ke korekturám má pouze jeho nadřízený pracovník.

4.3.3 Napájení zařízení

Napájení jednotlivých komponentů systému je zajištěno pomocí napájecích zdrojů. Celý systém je napájen z elektrické sítě 230 V/50 Hz a zajišťuje převod na stejnosměrné napětí 12 V. Samostatně jištěný přívod je proveden v rámci elektroinstalace budovy. Pro umísťování prvků napájecích zařízení platí technické podmínky výrobce.

4.4 Bezpečnostní analýza budovy

Provedení bezpečnostní analýzy areálu je základem každého bezpečnostního systému, a to ať už nově navrhovaného nebo při revizi toho stávajícího. Je naprosto nezbytným indikátorem, díky němuž se dozvíme, kde jsou slabá místa systému nebo naopak, kde je zabezpečení dostačující nebo dokonce naddimenzované. Při analýze posuzujeme charakter stavu současného zabezpečení, rozsah majetku a důležitost informací

vystavených riziku, pohyb osob a zaměstnanců, umístění budovy a zkušenosti s narušením zabezpečení z minulých období. Vypracování bezpečnostní analýzy musí předcházet jakémukoliv zavádění či rozšiřování nebo změně současného bezpečnostního systému.

Vzhledem k tomu, že se jedná o budovu samosprávy a tedy budovu veřejně přístupnou, nejde v určitém okamžiku zamezit vstupu osobám nepovolaným a nežádoucím. Dá se říci, že tato skutečnost nejvíce zvyšuje rizikovost budovy, a proto s ním musíme počítat a zapracovat, co nejdříve.

Obr. 19 Současná podoba budovy radnice

4.4.1 Analýza rizik a hrozeb v budově

Již v předchozí fázi praktické části jsem provedla analýzu současného stavu v daném objektu budovy místní samosprávy. Provedla jsem rozbor a popis stávajícího stavu prvků přístupového systému. Při posouzení zjištěného stavu jsem dospěla k závěru, že vybrané prvky poplachového systému jsou zaměřeny pouze na prostorovou a předmětovou ochranu. Perimetrická ochrana je řešena pouze částečně přístupovým systémem v místě vstupu. Vzhledem k tomu, že se jedná o velkou budovu, navíc veřejnosti přístupnou, vznikají zde slabá místa, která mohou být prostorem pro narušitele. Prioritou je tedy vytvoření účinné ochrany za použití poplachových systémů.

Jako zcela nevyhovující shledávám samotné zajištění vstupu do budovy. Tato velmi stěžejní část je ponechána v kompetenci lidského faktoru. Prakticky to znamená, že vstup do budovy zabezpečí pověřený pracovník, a to přepnutím režimu elektromechanických dveří na obousměrný provoz (dveře umožní vstup i odchod z budovy) z původního nočního jednosměrného provozu (dveře umožní pouze odchod z budovy, pro vstup zůstávají zavřené). Běžní zaměstnanci se vzhledem k nastavení práv na jejich přístupovém čipu dostanou do budovy až po tomto úkonu přepnutí na obousměrný provoz. Tou největší slabinou systému je skutečnost, že se takto do budovy nedostanou jen zaměstnanci před zahájením jejich pracovní doby a úředních hodin, ale již prakticky kdokoliv. Stejná situace nastává i po skončení pracovní doby a úředních hodin. Systém je opět závislý na lidském faktoru, tentokrát dveře na jednosměrný provoz přepínají pracovnice, které zajišťují úklid budovy. Sice jsou dána pravidla, kdy má dojít k uzamčení, resp. zamezení vstupu do budovy zvenčí, ale prakticky k tomu nikdy nedojde v přesně stanovený čas. Odchylky najdeme vždycky, a to buď v menší nebo větší míře. Navíc při neočekávané situaci může dojít k „uzamčení“ vchodu třeba až v hodinovém rozpětí. V práci dále navrhnu systém, který by pracoval nezávisle na lidech. Tím pádem se zamezí chybám a nedůslednostem způsobených lidským faktorem a od přesně stanovené doby nebude možnost vstupovat do budovy nepovolaným osobám.

Masivní zdivo zcela vyvrací průnik do budovy skrz něj. Rizikovým faktorem jsou spíše okna, kterých je v budově velký počet, a jež nejsou nijak zvlášť vyztužena a dokonce ani okna v přízemí nejsou osázena mřížemi.

Jako potenciální riziko vidím i možnost průniku do budovy přes nádvoří. Zde by stačilo pachatelům překonat zeď sousedící s vedlejším pozemkem, která je zčásti tvořena

postaveným domem a zčásti zahradou. Nepředpokládala bych proniknutí přes dům, ale právě přes tuto zahradu. Tím by byl zároveň umožněn přístup do celé budovy, protože dveře, které směřují na nádvoří, nejsou v žádném režimovém opatření, stejně tak výtah. Penetrace do budovy přes sousední zeď a nádvoří je sice nepravděpodobná, ale při provádění bezpečnostní analýzy musíme brát v úvahu všechny možnosti nebo je alespoň zmínit.

ACS je sice integrovaný s docházkovým systémem, ale zcela chybí napojení na CCTV. Určení oblastí pro optimalizaci a doplnění poplachových aplikací je nezbytné u objektů, které jsou z pohledu bezpečnosti rizikové, tzn. atraktivní pro potenciálního narušitele.

Tab. 2 SWOT analýza

SWOT ANALÝZA	
Silné stránky	**Slabé stránky**
bytelná konstrukce budovy - masivní zdivo	prostup do budovy přes dveře není dostatečně zajištěn
umístění v centru města	okna v přízemí nejsou opatřena žádným bezpečnostním prvkem
plášť budovy osvětlen veřejným osvětlením	vstup do budovy z nádvoří je zcela volný
	neexistuje centrální systém klíčů
bezprostřední blízkost služebny městské policie	absence CCTV
Příležitosti	**Hrozby**
vylepšení stávajícího přístupového systému	možnost vstupu do budovy nepovolaným osobám
doplnění systému o nové prvky	možnost zcizení dat, poškození majetku
zajištění větší bezpečnosti pracovníků	možnost napadení pracovníků
bezpečnost dat a informací	

4.5 Popis organizačního schématu

Vzhledem k tomu, že se jedná o rozsáhlou budovu s několika podlažími, bylo pro další práci nezbytně nutné vypracovat schémata těchto jednotlivých pater. Tímto výchozím materiálem byly půdorysy budovy, které jsou interní dokumentací. Půdorysy jsou vypracovány standardně, a pro potřeby této práce ne zcela vyhovující (viz přílohy). Pro zpracování organizace budovy bylo potřeba získat především přehlednost, tedy jednoduché, ale zároveň velmi přehledné situační mapky. Na těchto mapkách, respektive

organizačních schématech, jsou číselně označeny jednotlivé prostory v každém podlaží včetně vstupních otvorů; oken a dveří.

Na základě schematického rozčlenění všech podlaží bylo jednotlivým místnostem na těchto podlažích přiřazeno logické značení, které koresponduje s číslem podlaží. Dále pak posloužilo k následnému utřídění podle zón zabezpečení, resp. zón přístupu. Pro lepší názornost jsou tyto zóny vyznačeny barevně. V neposlední řadě bylo třeba označit dveře (dveřní zámky), pokud místnost disponuje více než jedněmi dveřmi. Tyto přehledy slouží jako podklad pro vypracování přehledu pro přidělení identifikátorů (klíčů) konkrétním osobám podle stanovených přístupových práv, viz kapitola 6. Každé schéma je také doplněno vysvětlivkami s piktogramy.

Za každým schématem následuje tabulka, která každý očíslovaný prostor označuje i slovním popisem.

Tab. 3 Rozdělení a popis zón přístupu

ZÓNY PŘÍSTUPU		
Zóna	**Označení**	**Popis**
zelená	Zóna bez omezení vstupu	prostory volně přístupné veřejnosti i mimo pevnou pracovní dobu (PPD*) referentů
žlutá	Zóna I. stupně omezení	prostory volně přístupné veřejnosti v pracovní době za přítomnosti referenta; místnost se po dobu nepřítomnosti referenta uzamyká
oranžová	Zóna II. stupně omezení	prostory s režimovým opatřením, pohyb pouze pověřených osob nebo vstup veřejnosti na základě povolení vstupu, případně s doprovodem pověřené osoby
červená	Zóna III. stupně omezení	prostory zcela nepřístupné veřejnosti, pohyb pouze pověřených osob s autorizací vstupu (záznam o vstupu)

*PPD - pevná pracovní doba

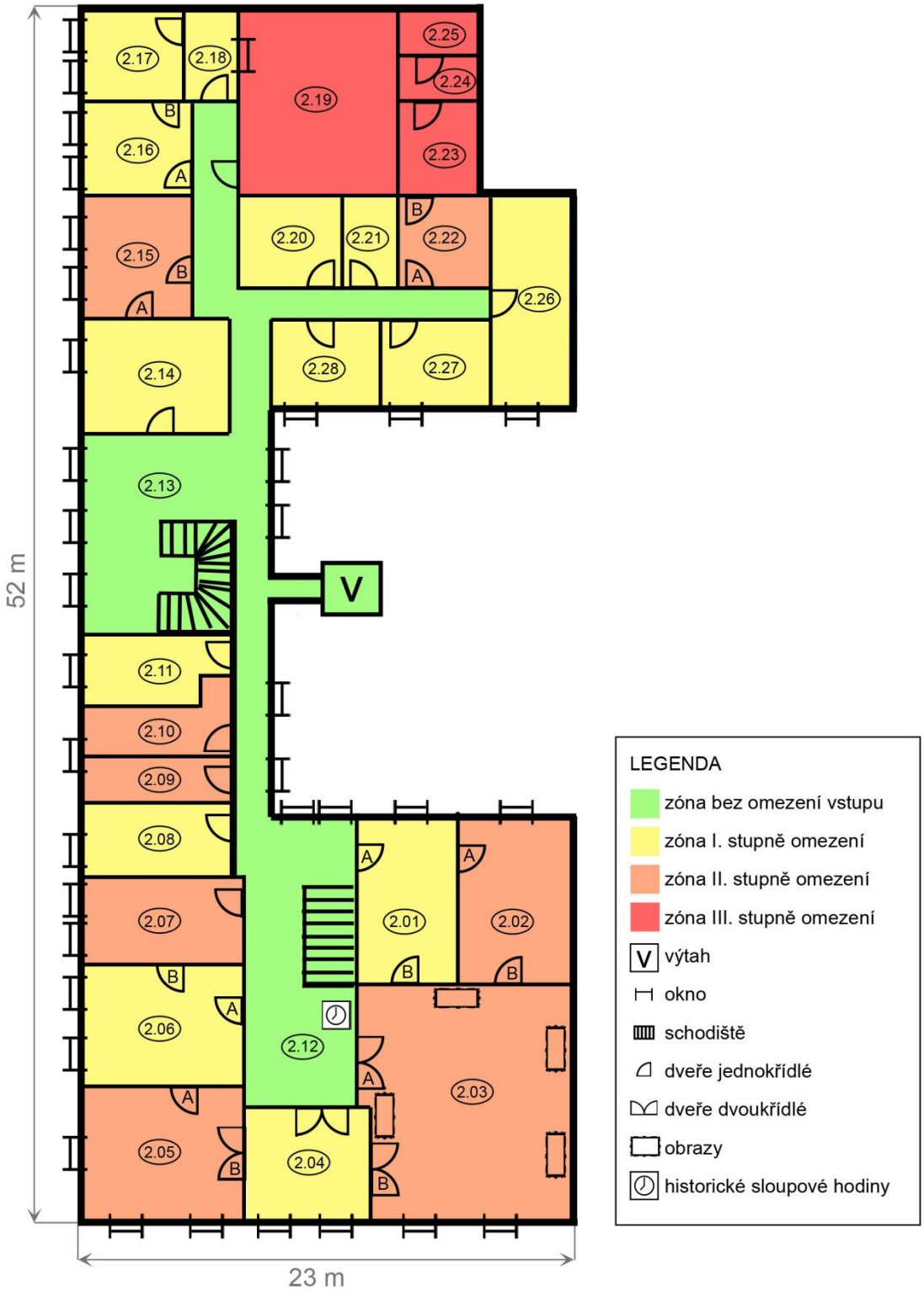
PO	8 - 17:00 h	ÚŘEDNÍ DEN
ÚT	8 - 14:30 h	
ST	8 - 17:00 h	ÚŘEDNÍ DEN
ČT	8 - 14:30 h	
PÁ	8 - 14:00 h	

4.6 Organizační schéma budovy

Obr. 20 Půdorys 1. nadzemního podlaží

Tab. 4 Popis 1. nadzemního podlaží

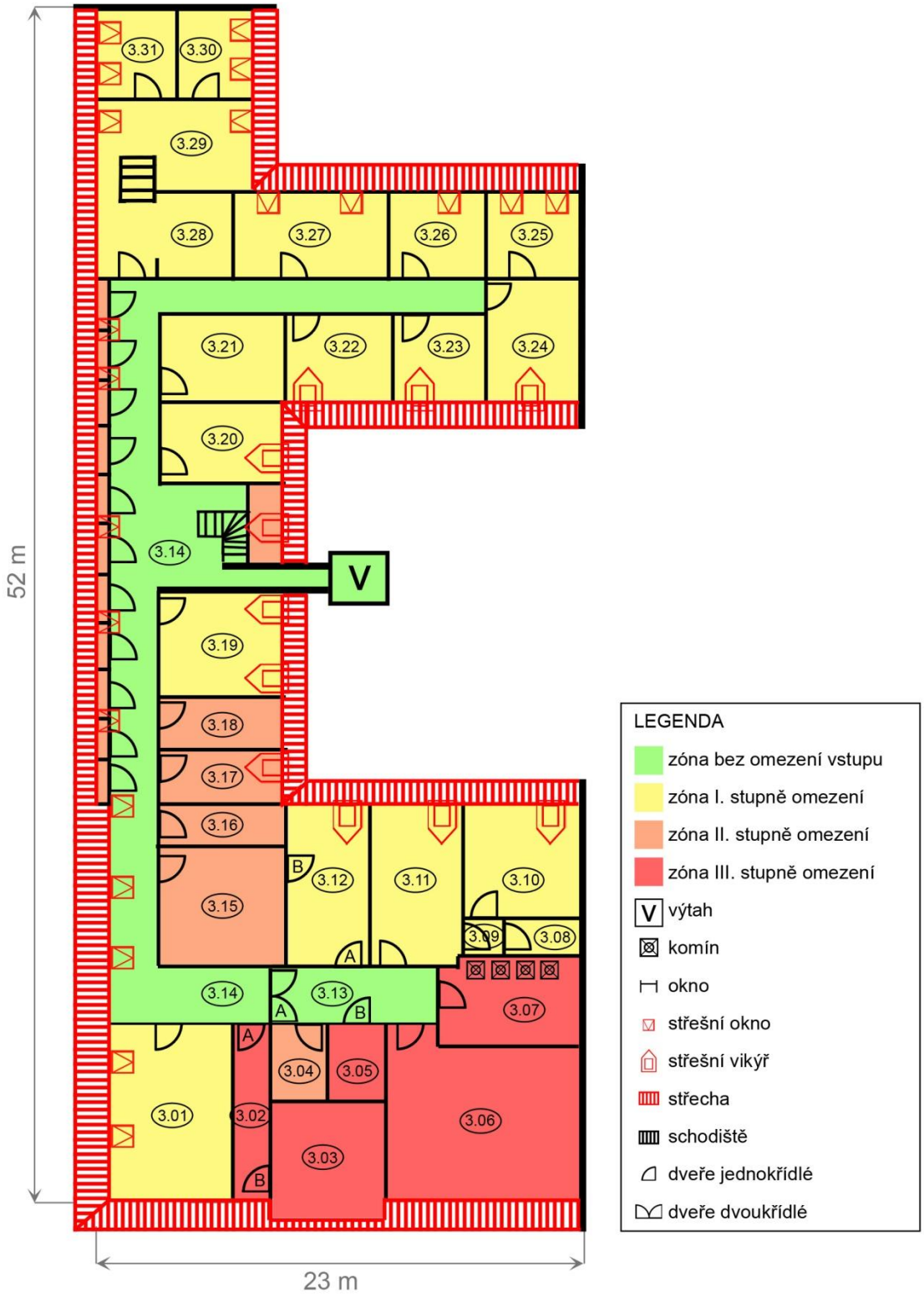
1. NADZEMNÍ PODLAŽÍ	
Označení	**Účel prostoru**
1.01	Vstupní prostor
1.02	Chodba
1.03	Vstupní prostor boční
1.04	Nádvoří
1.05	WC
1.06	Odbor správní - matrika
1.07	Odbor správní - doručovatelky
1.08	Odbor správní - podatelna
1.09	Odbor správní - evidence obyvatel
1.10	Odbor správní - kartotéka
1.11	Odbor správní - občanské průkazy, cestovní doklady
1.12	Odbor správní - občanské průkazy, cestovní doklady
1.13	Odbor správní - kancelář
1.14	Odbor správní - kancelář
1.15	Zasedací místnost
1.16	Čajová kuchyně
1.17	Archiv
1.18	Předsíň
1.19	WC ženy
1.20	WC muži
1.21	Odbor kanceláře tajemníka - sklad čisticích prostředků
1.22	Odbor kanceláře tajemníka - sklad kancelářských potřeb
1.23	Předsíň
1.24	Odbor správy majetku města - dílna údržby
S	Studna
V	Výtah
X1	Pronajatý prostor 1
X2	Pronajatý prostor 2



Obr. 21 Půdorys 2. nadzemního podlaží

Tab. 5 Popis 2. nadzemního podlaží

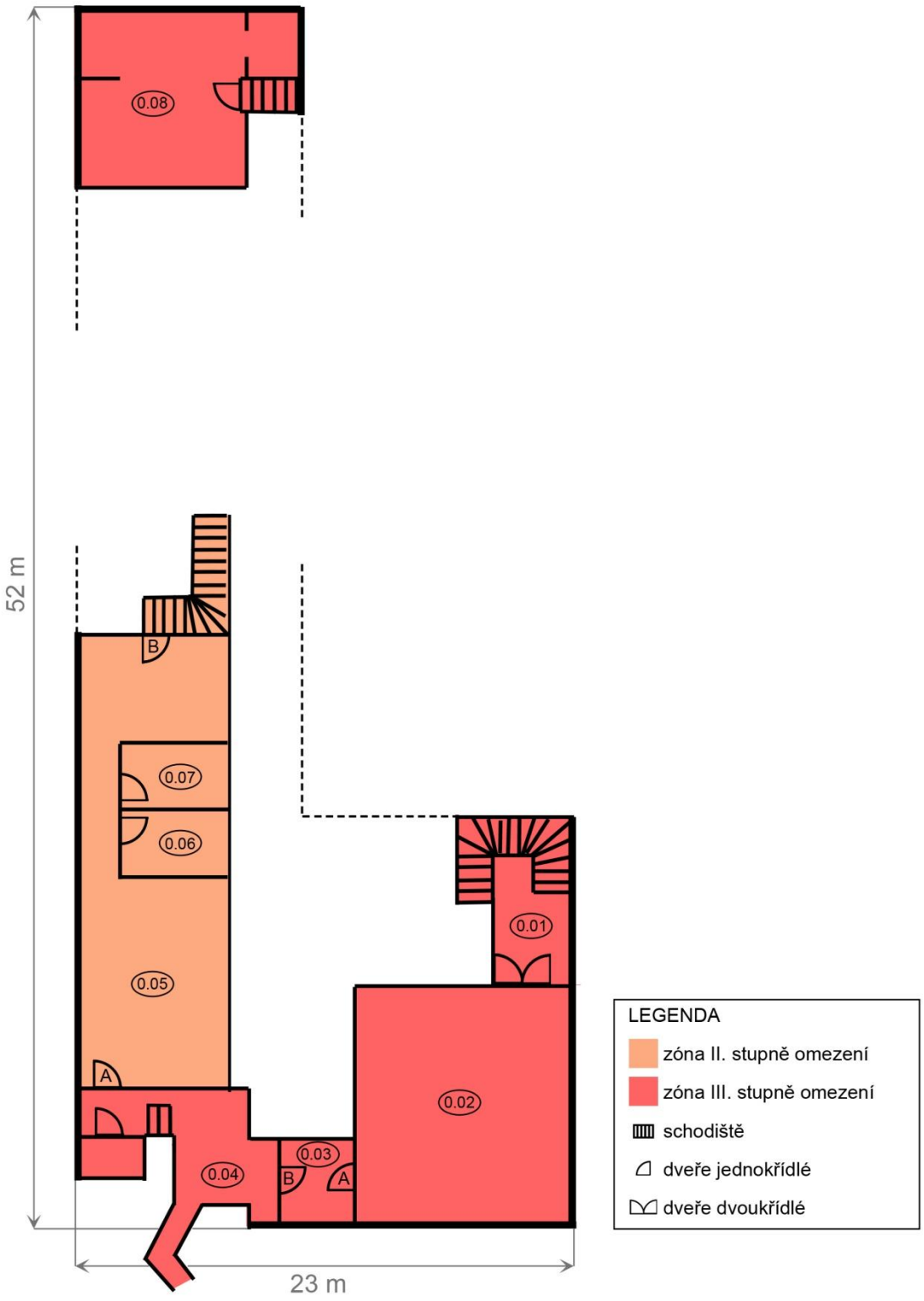
2. NADZEMNÍ PODLAŽÍ	
Označení	**Účel prostoru**
2.01	Odbor kanceláře tajemníka - sekretariát
2.02	Kancelář místostarosty
2.03	Zasedací místnost
2.04	Odbor kanceláře tajemníka - tisková mluvčí
2.05	Kancelář starosty
2.06	Odbor kanceláře tajemníka - sekretariát
2.07	Kancelář místostarosty
2.08	Odbor finanční - vymáhání pohledávek
2.09	WC muži
2.10	WC ženy
2.11	Odbor finanční - daně a poplatky
2.12	Chodba
2.13	Chodba
2.14	Odbor kanceláře tajemníka - sekretariát
2.15	Odbor kanceláře tajemníka - kancelář tajemníka
2.16	Odbor finanční - kancelář
2.17	Odbor finanční - kancelář
2.18	Odbor finanční - kancelář vedoucího
2.19	Terasa
2.20	Odbor finanční - správa daní
2.21	Odbor kanceláře tajemníka - mzdová účtárna
2.22	Kopírovací místnost
2.23	Archiv oddělení informatiky
2.24	Servrovna
2.25	Servrovna
2.26	Odbor kanceláře tajemníka - kancelář informatiky
2.27	Odbor kanceláře tajemníka – GIS, MAN-UB
2.28	Kancelář - interní audit



Obr. 22 Půdorys 3. nadzemního podlaží

Tab. 6 Popis 3. nadzemního podlaží

3. NADZEMNÍ PODLAŽÍ	
Označení	**Účel prostoru**
3.01	Odbor rozvoje města - investiční technik
3.02	Chodba
3.03	Věž
3.04	Kopírovací místnost
3.05	Archiv
3.06	Archiv
3.07	Kotelna
3.08	Odbor rozvoje města - oddělení dotací
3.09	Odbor rozvoje města - oddělení dotací
3.10	Odbor rozvoje města - oddělení dotací
3.11	Odbor rozvoje města - oddělení dotací
3.12	Odbor rozvoje města - kancelář
3.13	Chodba
3.14	Chodba
3.15	Odbor rozvoje města - kancelář vedoucího
3.16	Čajová kuchyně
3.17	WC muži
3.18	WC ženy
3.19	Odbor kanceláře tajemníka - zvláštní úkoly
3.20	Odbor finanční - přestupkové řízení
3.21	Odbor finanční - přestupkové řízení
3.22	Odbor správy majetku města - technik BOZP, osvětlení
3.23	Odbor správy majetku města - místní komunikace
3.24	Odbor kanceláře tajemníka - oddělení právní
3.25	Odbor kanceláře tajemníka - oddělení právní - vedoucí
3.26	Odbor správy majetku města - kancelář
3.27	Odbor správy majetku města - bytové záležitosti
3.28	Odbor správy majetku města - sekretariát
3.29	Odbor správy majetku města - správa majetku
3.30	Odbor správy majetku města - evidence nemovitostí
3.31	Odbor správy majetku města - kancelář vedoucího



Obr. 23 Půdorys podzemního podlaží

Tab. 7 Popis podzemního podlaží

PODZEMNÍ PODLAŽÍ	
Označení	**Účel prostoru**
0.01	Chodba
0.02	Odbor finanční - archiv
0.03	Sklep
0.04	Místnost pro vodoměr
0.05	Sklepení
0.06	WC muži
0.07	WC ženy
0.08	Sklep se studnou

4.7 Režimová opatření objektu

Přístupový systém slouží jako systém zabezpečení vstupu do budovy. Vstupem jsou vstupní dveře do budovy. Skládá se z kontaktních snímačů docházkových čipů, řídicích dveřních jednotek, napájecích zdrojů a externích zařízení (pohony dveří, elektrické zámky). K nastavení přístupových oprávnění slouží verze softwaru Advent, která obsahuje základní systémové funkce.

Tab. 8 Rozdělení přístupových práv z hlediska současného režimového opatření

Stupeň práva přístupu	Kdo	Vstup do budovy
žádný	veřejnost, návštěvy	po manuálním přepnutí dveří na obousměrný provoz ←→
standardní	zaměstnanci	po manuálním přepnutí dveří na obousměrný provoz ←→
úplný	vybraní zaměstnanci, vedoucí pracovníci	kdykoliv, bez omezení

Vstup do areálu je po manuálním přepnutí dveří na obousměrný provoz prakticky možný komukoliv v průběhu dne a pracovního týdne. Znamená to tedy, že se do budovy v tuto dobu dostanou nejen pověření pracovníci, ale bohužel i cizí osoby, neboť v tuto dobu projdou bez nějakých překážek. Zaměstnanci se musí identifikovat čipovým identifikačním

médiem (iButton) na čtečce, která je umístěna na docházkovém terminálu u obou vstupních dveří, což ale není podmínkou vstupu. Docházkové terminály jsou tedy dva s upevněním na zdech. Pro zaměstnance se standardním nastavením čipu je umožněn vstup v čase od 6:00 hodin, kdy dojde k manuálnímu přepnutí dveří. Zaměstnanci, kteří mají vyšší přístupová práva, tedy nastavený přístup úplný, si mohou vstupní dveře otevřít prostřednictvím přístupového čipu kdykoliv. Samozřejmě každý průchod je evidován a zaznamenám do paměti s možností pozdějšího zjištění průchodu v konkrétním čase a konkrétní osobou.

5 NÁVRH NOVÉHO SYSTÉMU A REŽIMOVÝCH OPATŘENÍ

5.1 Návrh nového systému

Na základě bezpečnostní analýzy rizik a hrozeb byla zjištěna slabá a silná místa stávajícího zabezpečení areálu a ACS. Díky tomu můžeme zjištěné nedostatky odstranit či alespoň výrazně eliminovat, zajistit a navrhnout novou koncepci celkového zabezpečení. Tento návrh bude zaměřen na optimalizaci ACS, nastavení nových pravidel přístupu a celkově zvýšení bezpečnosti budovy jako takové a obzvláště jejich zaměstnanců.

Základním kritériem pro návrh ACS je zcela jistě význam a povaha chráněného objektu, stavební struktura, hodnota majetku uvnitř objektu, míra rizika pro napadení a další faktory, které mají vliv na výběr ACS. Vzhledem k tomu, že se nacházíme v samotném centru památkové zóny a tudíž i v památkové budově, musíme respektovat pravidla týkající se i této oblasti.

Nové organizační schéma představuje schéma s rozmístěním kamer CCTV, a proto je uváděno až v kapitole vztahující se k tomuto tématu. V budově radnice dosud nebylo zpracováno žádné organizační schéma mimo to, které je uvedeno při popisu objektu a které jsem vypracovala pro potřeby této práce. K původnímu schématu bych dodala, že nebyly striktně dodržovány zóny s omezením vstupu.

5.2 Nová režimová opatření

Zavedením kvalitního a propracovaného režimového opatření můžeme takřka ihned zvýšit ochranu objektu, majetku i osob, dalo by se říci, bez jakékoliv počáteční investice. Předpokladem je však striktní dodržování navržených pravidel. Na úrovni použití závisí výsledná účinnost.

Správné režimové opatření chápu jako soubor organizačně administrativních opatření a postupů, které zajišťují požadované podmínky pro smysluplnou funkci zabezpečovacího systému a jeho sladění s provozem chráněného objektu.

5.2.1 Vnější režimová opatření

Vnější režimová opatření se týkají především vstupních a výstupních podmínek z chráněného objektu, tj. prostoru, kudy se osoby dostávají do objektu a kudy jej také opouštějí.

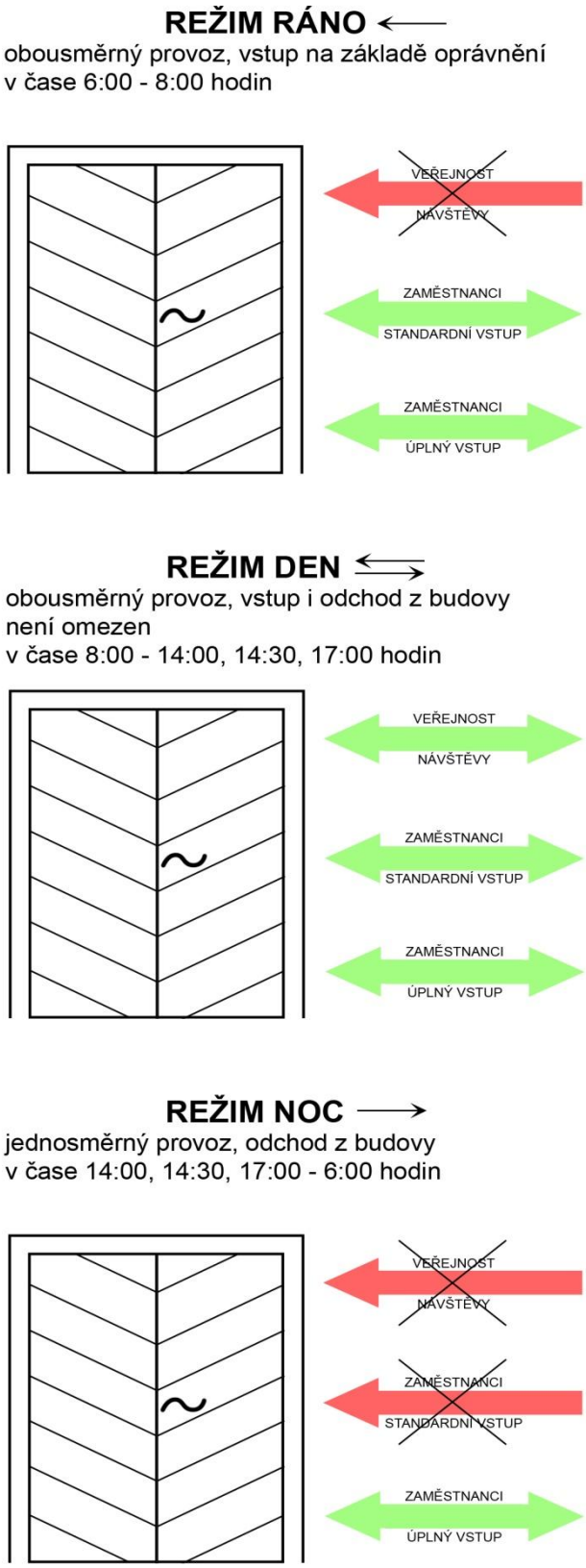
Přístupový systém do budovy navrhuji oprostit od lidského faktoru a přejít na **automatický časový režim**, tedy režim řízený přístupovým systémem. V tomto momentu již nebude nutné, aby byl pověřený pracovník každý pracovní den v 6:00 hodin na místě a otevřel, resp. přepnul režim elektromechanických dveří na obousměrný provoz (režim DEN ←→) z původního nočního jednosměrného provozu (režim NOC →). Každý zaměstnanec by se tak do budovy v pracovním týdnu v režimu DEN ←, resp. nově v režimu RÁNO dostal bez potíží, ale dveře za ním by se zavřely a byl by tak zamezen průchod neoprávněným osobám, např. občanům. Tím pádem bude zamezeno vstupu cizích osob, což značně zvýší bezpečnost budovy. Při aplikaci tohoto systému se občané do budovy dostanou pouze v době pevné pracovní doby zaměstnanců. V tomto čase bude automaticky nastaven obousměrný provoz dveří (režim DEN ←→).

Tab. 9 *Rozdělení přístupových práv z hlediska nového režimového opatření*

Stupeň práva přístupu	Kdo	Vstup do budovy
žádný	veřejnost, návštěvy	pouze v pevné pracovní době zaměstnanců
standardní	zaměstnanci	pouze při přepnutí automatického časového režimu (režim RÁNO ←, režim DEN ←→)
úplný	vybraní zaměstnanci, vedoucí pracovníci	kdykoliv, bez omezení

Ta samá situace nastávala v době skončení pevné pracovní doby. Dveře na jednosměrný provoz přepínali pracovnice zajišťující úklid budovy. S novým systémem bude opět toto přepnutí řešeno automatickým časovým režimem a bude zajištěno v přesně určený čas. V tomto případě skončením pevné pracovní doby. Od tohoto okamžiku se do budovy nedostane nikdo cizí (vstup je zakázán), odchod z budovy je povolen nastavením jednosměrného provozu.

Tento princip je jednoduchý, ale přesto velice účinný. Navíc není třeba instalovat žádný nový systém, ale pouze upravit fungování stávajícího.



Obr. 24 Schéma nového režimového opatření

5.2.2 Vnitřní režimová opatření

Vnitřní režimová opatření se týkají především omezení pohybu osob v objektu jen v určitém prostoru, v určité oblasti. Jde o omezení vstupu do určitých prostor pouze pro určité pracovníky.

Z vnitřních režimových opatření je třeba dodržovat důslednost v uzamykání jednotlivých kanceláří a míst, kam zaměstnanci vstupují. Vzhledem k návrhu implementace systému generálního hlavního klíče budou mít vždy při ruce klíč, kterým otevřou dveře, kam mohou vstupovat.

6 NÁVRH TECHNICKÝCH PROSTŘEDKŮ

Ochrana, jak by se v obecném pojetí dala nazvat, je vytvořením bezpečného prostředí pro daný subjekt. Abychom mohli navrhnout konkrétní ochranu, musíme detailně poznat předmět ochrany, tedy objekt, který chceme chránit a specifikovat, co je cílem ochrany, tedy proti čemu jej chránit, definovat předpokládané hrozby a nebezpečí.

Samotná realizace ochrany představuje návrh a sladění všech dostupných prostředků, které zajistí požadovanou bezpečnost. Prostředky použité pro realizaci ochrany jsou přímo tím bezpečnostním systémem a jejich souhrn představuje integrovaný celek. Tímto integrovaným celkem zajistíme bezpečnost osob, informací a majetku. Ochrana osob by samozřejmě měla být všude označena nejvyšší prioritou. Následuje ji ochrana informací a pak ochrana majetku.

Při návrhu technických prostředků ochrany musíme mít na paměti tři základní pravidla, a to ta, že **neexistuje absolutní ochrana.** Berme v úvahu, že každá ochrana může být překonána. **Jedna skupina ochran nic neřeší** - realizujme ochranu vždy v integrovaném celku, jen tak bude zajištěna požadovaná účinnost. **Technické prostředky nenahradí člověka** - ostraha dokáže posoudit, zda vyvolaný poplach byl planý či nikoliv a provede následné kroky.

V tomto oddíle navrhnu technické prostředky pro zajištění veškerých požadovaných funkcí systému.

6.1 Současné prvky objektu a návrh opatření

Mezi klasickou ochranu zábrannými systémy k zajištění příslušného objektu zcela jistě navrhuji použití mechanických zařízení pro účely ochrany. Konkrétně v tomto případě půjde o výměnu dveřních cylindrických vložek. Dá se říci, že tato forma je nejrychlejším a nejlevnějším řešením a můžeme se s ní prakticky setkat v každém objektu.

Jak nám ukazuje celý historický vývoj i současné zkušenosti, prostředky klasické ochrany nejsou schopny chráněné objekty a prostory zabezpečit beze zbytku. Hovoříme zde o tzv. **zpožďovacím faktoru**, který určuje, jak dlouho je konkrétní prostředek klasické ochrany schopen odolávat kvalifikovanému napadení dostupnými nástroji a metodami.

6.1.1 Klasické vstupní dveře

Rozhodně nemohu opomenout největší vstupní otvor do budovy, kterým jsou masivní historické dvoukřídlé dřevěné dveře doplněné z vnitřní strany identifikačním přístupovým systémem. Dveře jako takové jsou jedním z nejdůležitějších stavebních otvorů. Jsou tvořeny ze zárubně, která je pevnou součástí stavby a tím zajišťuje, že se nedá běžný způsobem vyrazit. Dále obsahuje dveřní křídla, panty, zámek a historické kování. Na dveřní systémy existuje velké množství zabezpečovacích prvků, které poskytují vyšší standard zabezpečení. Dveře budou zahrnuty do systému generálního hlavního klíče. Tento systém je založen na principu, že každou zámkovou vložku v systému může otevřít jen klíč s předem definovanou pravomocí. Pro jednoznačnou identifikaci vstupu do jednotlivých zón, budou vstupy do těchto zón opatřeny elektromechanickou zámkovou vložkou, která obsahuje čtecí zařízení. Tyto vložky plní funkci elektronického přístupového systému. Zabezpečí jednoznačnou identifikaci vstupu dané osoby přiřazeným kódovaným klíčem a uchová o tom záznam (čas, datum). Všechny klíče generálního systému budou opatřeny jednoznačným elektronickým identifikátorem. Tento identifikátor požadovaný vstup do zóny povolí nebo zamítne. Výhodou je kontrola o použití dveří díky možnosti vyvolání historie.

Obr. 25 Hlavní vstupní dveře

Vzhledem k návrhu aplikace automatického časového režimu na dveře je u těchto nutné přidat systém zajišťující zavření dveří, tzv. brano, které bude uzpůsobeno na váhu těchto

dveří. Současně s tím budou dveře opatřeny jazýčkovým spínačem, který bude indikovat stav dveří otevřeno/zavřeno, aby nenastal případ, kdy dveře nebudou řádně uzavřeny. V případě, že dveře nebudou řádně uzavřeny, zabezpečí tato smyčka akustickou signalizaci tohoto stavu.

Systém dovření dveří, tzv. brano, bude instalováno na všech dveřích, kde požadujeme elektronické snímání průchodů, a to z toho důvodu, aby se dveře vždy dovřely při průchodu oprávněného pracovníka a nezůstaly tak otevřeny pro případ neoprávněného vstupu člověka bez příslušných přístupových práv k těmto dveřím.

6.1.2 Elektromechanické vstupní dveře

Součástí vstupního systému z boční strany budovy jsou elektromechanické vstupní dveře, které jsou taktéž doplněny o přístupový systém, který se nachází jak z vnější, tak z vnitřní strany. Na dveřích navrhuji instalovat vstupní časový zámek, který bude v naprostém souladu s pevnou pracovní dobou.

Obr. 26 Vstupní dveře boční

6.1.3 Okna budovy

Okna, obdobně jako dveře, jsou jedním z kritických míst budov. Jejich jednoduchým rozbitím se pachatel může lehce dostat do vnitřních prostor budovy. Existuje velké množství bezpečnostních prvků, kterými lze okna zabezpečit proti neoprávněnému vniknutí.

Rozšířenou formou ochrany oken jsou **mříže**, které svou bytelností zajišťují maximální bezpečnost. Musí být však pevně ukotveny ve zdi a celá konstrukce musí být z kvalitního materiálu, který se nedá roztáhnout a je stabilní. Další možností ochrany skleněných ploch jsou **bezpečnostní fólie.** Velkou výhodou je rychlá montáž, při které se na vnitřní stranu

skleněné plochy nalepí tenký film polyesteru, který je zcela průhledný a vysoce světlopropustný. Bezpečnostní fólie zpomalí postup zloděje, zamezí prohození předmětů oknem, chrání proti účinku tlakových vln a také dokáže zpomalit šíření požáru.

Obr. 27 Skleněná plocha opatřená bezpečnostní fólií

Využití bezpečnostních fólií je poměrně efektivním bezpečnostním opatřením, když vezmeme v úvahu cenovou dostupnost, rychlost montáže a účinnost. Optimálním řešením by bylo opatřit bezpečnostními fóliemi všechna okna v 1. nadzemním podlaží, která jsou umístěna přibližně 1 metr nad úrovní venkovního terénu. Pokud by se neumísťovala na všech oknech, tak minimálně v kancelářích v tomto podlaží, které jsou v době nepřítomnosti střeženy alarmem z důvodu evidence, zpracování a vydávání cestovních dokladů a občanských průkazů.

Volila bych bezpečnostní fólie s atestem na kategorii odolnosti, která je i alternativou funkční mříže ve smyslu pojistných podmínek některých pojišťoven. Tyto bezpečností fólie můžeme pořídit za cca 650 Kč/m^2, montáž 300 Kč/m^2.

Tvrzená nebo vrstvená skla jsou další možností ochrany oken. Výroba tvrzených skel probíhá speciální technologií, která zajistí v celé ploše trvalé pnutí a pokud dojde k rozbití, rozpadne se na velký počet malých neostrých úlomků. Vrstvené sklo je vyráběno sendvičovou metodou, kdy se mezi dvě odolná skla vloží bezpečnostní fólie, která tak mnohonásobně zvýší odolnost, dokonce i proti nárazu ocelovou koulí či kladivem.

6.2 Technická ochrana novými prvky

Technická ochrana představující poplachové systémy podporuje ochranu klasickou a je nejspolehlivější a nejhůře překonatelnou z hlediska dnešních požadavků i technických možností. Technickou ochranu můžeme označit jako detekční systém, který zajišťuje a předává informace o situaci v chráněném objektu či prostoru a o jeho případné napadení.

Můžeme říct, že technická ochrana podstatně zvyšuje efektivnost ochrany klasické a také ochrany fyzické. Nicméně fyzickou ostrahu uvedeného objektu neaplikuji nejen z hlediska finančního, neboť fyzická ochrana se řadí ze všech typů ochran mezi nejdražší, a její použití ani s uplynulým časem neklesá z důvodu stálých nákladů na platy.

6.2.1 Systém Generálního hlavního klíče

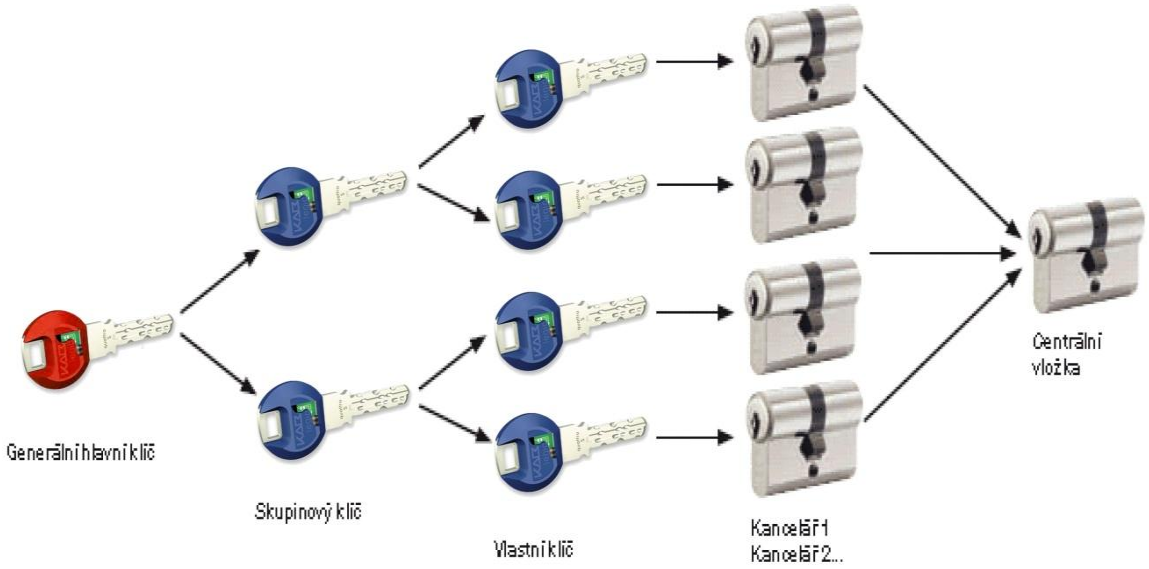
Rychlým, spolehlivým a přitom jednoduchým zabezpečením budovy je využití systému Generálního hlavního klíče. Jedná se o sofistikované systémy pro uzamykání a jednoduché ovládání uzamykacích systémů, které jsou v současnosti technologickou špičkou. Navíc nespornou výhodou je možnost uzamknutí celé budovy jediným klíčem, není potřeba tak stále s sebou nosit velké svazky klíčů. I přesto, že se uzamkne celá budova jediným klíčem, stále se jedná o originál pro každé dveře. Jde o realizaci přístupového práva pomocí elektromechanického klíče, který má **charakter identifikátoru** (např. jako karta) a obsahuje přesné identifikační prvky. Každý klíč má pevný mechanický kód podle nastavených pravomocí (viz tabulka přidělení identifikátorů a přístupových práv). Pověřený pracovník nahraje kódy do elektromechanických zámků, které jsou umístěné na klíčových místech budovy (např. hlavní vchod, vstup do archivu, atd.).

Generální hlavní klíč (GHK) - v rámci systému umožňuje uzamknout všechny vložky. Tento klíč zpravidla vlastní osoba nejvýše postavená v hierarchii podniku. A další klíč - záložní bývá uložen v trezoru. Tímto klíčem je možné bez omezení procházet všemi vstupy v celém systému.

Hlavní klíč (HK) - tento klíč uzamyká všechny vložky v rámci jednoduššího uzamykacího systému. V uzamykacím systému s GHK se HK stává skupinovým klíčem. V našem případě je tedy hlavní a generální hlavní klíč shodný.

Skupinový klíč (SK) - uzamyká v rámci uzamykacího systému s GHK určitou skupinu vložek (např. určité oddělení).

Vlastní klíč (VK) - tento klíč je poslední v hierarchii oprávnění. Vlastní klíč uzamyká jen určitou vložku, k tomu případně i centrální vložku.



Obr. 28 Struktura systému GHK

Z obrázku je patrné, kde se v klíči-identifikátoru nachází část mechanická a kde elektronická.

Celý systém takto můžeme uzamknout jediným klíčem v závislosti na příslušných oprávněních. Klíče v systému nesou dvě kódové označení. 1. Mechanické - určuje pravomoc ke vstupu do jednotlivých prostor, které nejsou opatřeny elektronickou čtečkou čipu. 2. Elektronický identifikátor - tento elektronický identifikátor určuje pravomoc ke vstupu do jednotlivých zón. Vstupy do zón jsou zabezpečeny dveřní vložkou s integrovanou čtečkou elektronického identifikátoru. Čtecí zařízení zaznamená jednoznačný elektronický kód klíče, datum a čas, kdy do prostoru vstoupil.

Přehled kladů a záporů při využití generálního hlavního klíče:

Výhody +

- evidence klíčů,
- stanovení přístupů a práv,
- zvýšení zabezpečení budovy,
- odpovědnost za svěřené prostory a majetek v nich,
- možnost napojení na docházkový systém,
- administrace systému z jednoho místa,

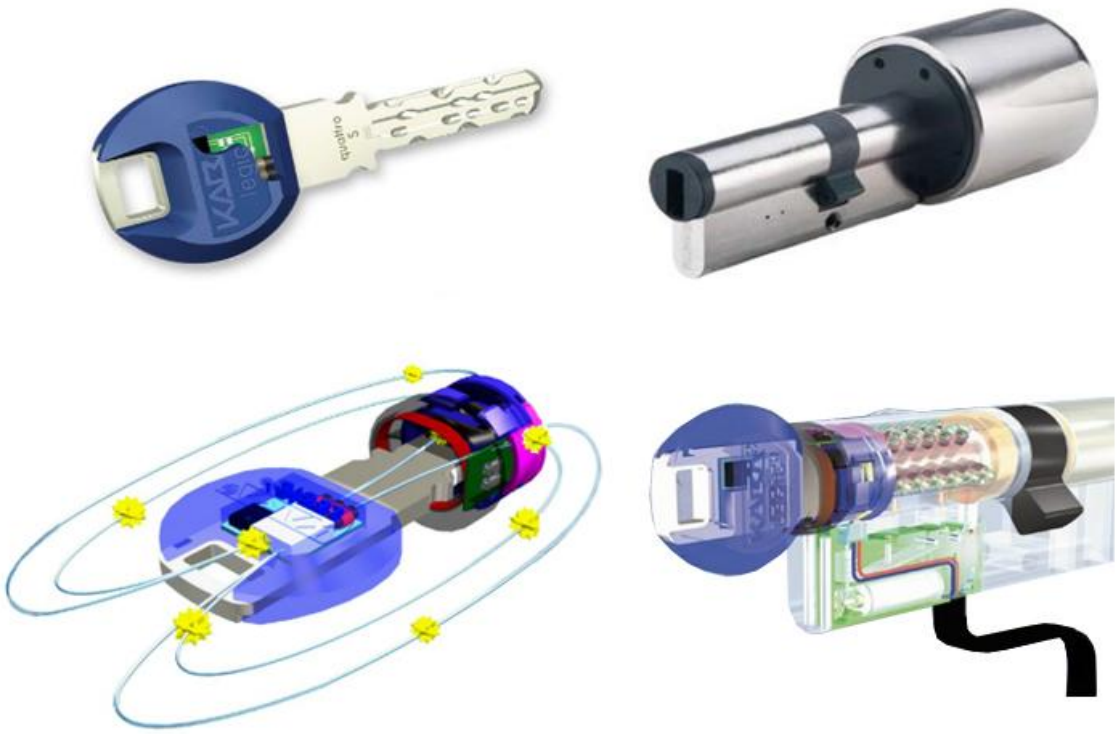
- komfort a jistota.

Nevýhody -

- vyšší cena vložky,
- vyšší cena klíče,
- vyšší náklady při ztrátě klíče.

6.2.2 Systém mechatronického klíče

Mechanický systém GHK se dá vylepšit na mechatronický klíč integrací mikročipu (transponderu). Jedná se tedy o mechanický klíč vybavený mikročipem. Každý transponder je unikátní a není kopírovatelný. Tato dodatečná elektronická kontrola vstupů pomocí transponderu umožňuje jednoduchou a flexibilní organizaci oprávnění vstupů a zvyšuje tak celkovou bezpečnost systému. Elektronické identifikátory je možno integrovat například do karet nebo čipů. Bezpečnost uzamknutí je na vysoké úrovni, umožňuje bezkontaktní přenos dat a zajišťuje signalizaci výměny baterky. Baterie 1,3 nebo 3 V je umístěna v zámkové vložce. Výdrž baterií udána výrobcem je dva roky.



Obr. 29 Průřez klíče s identifikátorem [18]

Využitím těchto prvků budu mít kontrolu nad vstupy do prostor (například archiv, zasedací místnost, místnost se servery), které chci sledovat, resp. v případě potřeby si stáhnu historii

z těchto zámků. Tyto informace dříve nikdo nesledoval, protože k tomu ani nebyly vyvinuté možnosti.

Společnou výhodou mechanických a mechatronických prvků je **bezpečnost investice**, kdy mechanické uzamykací systémy je možné kdykoliv rozšířit o elektronickou kontrolu vstupů, a to vše bez dodatečné nákladné kabeláže. Je tam připravena půda pro možnost rozšíření v budoucnosti.

V těchto systémech mě nejvíce zaujala nabídka společnosti KABA, která se na trhu vyskytuje dlouhou řadu let a je známa po celém světě kvalitou svých produktů, konkrétně systém s mikročipem - EloLegic. Samozřejmě není nutné realizaci provádět přímo s výrobky této značky, protože nepatří k nejlevnějším, ale jsou vysoce kvalitní a zajišťují ochranu klíče-identifikátoru patentem. Nicméně pro potřeby této práce bude dále využíván pojem EloLegic, který právě představuje elektronický systém, který je navržen použít.

Obr. 30 Čipová technologie s EloLegic [18]

Přidělení identifikátorů přístupových práv systému konkrétním osobám

Pro jasný a srozumitelný přehled přístupových práv byla vytvořena tabulka, ve které je vymezen přístup konkrétního pracovníka dle jeho funkce do konkrétních míst přístupu. Právo přístupu je nadefinováno přímo na číslo dveří, resp. konkrétní vložku každých dveří - mechanická část. Každý klíč je vybaven mikročipem, tedy nosičem, ve kterém jsou nadefinována práva pro konkrétní dveře osazené čtečkou čipů - elektronická část. Tyto čtečky umožňují vést záznam o jednotlivých průchodech. Funkce zaměstnance určuje, kolik stejných klíčů bude na základě stejných přístupových práv vyrobeno. Nejvyšší množství povolených vstupů mají samozřejmě vedoucí pracovníci.

Vzhledem k velikosti celé tabulky je tato uváděná v příloze. Zde je pro názornou představu ponechána její výseč, ze které je patrné, který pracovník si může otevřít příslušné dveře.

				Počet klíčů	1	1	2	1	1	2	2	2	2	2
				Klíče	Generální klíč	Starosta	Místostarosta	OKT - tajemník	OKT - sekretariát starosty	OKT - sekretariát místostarostů	OKT - sekretariát tajemníka	OKT - tisková mluvčí	OF - vymáhání pohledávek	OF - správa daní a poplatků
Poř. číslo	Číslo dveří	Označení prostoru	Rozměr vložky - A+B, typ zámku (mm)											
1	1.01	Vstupní prostor - HLAVNÍ VCHOD	EloLegic		X	X	X	X	X	X	X	X	X	X
2	1.02	Chodba	30+35,5		X	X	X	X	X	X	X	X	X	X
3	1.03A	Vstupní prostor boční - BOČNÍ VCHOD	EloLegic		X	X	X	X	X	X	X	X	X	X
4	1.03B	Vchod na nádvoří	30+35,5		X	X	X	X	X	X	X	X	X	X
5	1.05	WC	30+35,5		X	X	X	X	X	X	X	X	X	X
6	1.06	Odbor správní - matrika	30+35,5		X			X						
7	1.07	Odbor správní - doručovatelky	30+35,5		X			X						
8	1.08	Odbor správní - podatelna	30+35,5		X	X	X	X	X	X	X			
9	1.09	Odbor správní - evidence obyvatel	30+35,5		X			X						
10	1.10	Odbor správní - kartotéka	30+35,5		X			X						
11	1.11A	Odbor správní - občanské průkazy, cestovní doklady	30+35,5		X			X						
12	1.11B	Odbor správní - občanské průkazy, cestovní doklady	30+35,5		X			X						
13	1.11C	Odbor správní - občanské průkazy, cestovní doklady	30+35,5		X			X						
14	1.12	Odbor správní - občanské průkazy, cestovní doklady	30+35,5		X			X						
15	1.13	Odbor správní - kancelář	30+35,5		X			X						
16	1.14A	Odbor správní - kancelář	30+35,5		X			X						
17	1.14B	Odbor správní - kancelář	30+35,5		X			X						
18	1.15A	Zasedací místnost	30+35,5		X	X	X	X	X	X	X			
19	1.15B	Zasedací místnost	30+35,5		X	X	X	X	X	X	X			
20	1.15C	Zasedací místnost	30+35,5		X	X	X	X	X	X	X			
21	1.15D	Zasedací místnost	30+35,5		X	X	X	X	X	X	X			
22	1.16	Čajová kuchyně	30+35,5		X	X	X	X	X	X	X	X	X	X
23	1.17	Archiv	EloLegic		X	X	X	X	X	X	X	X		
24	1.18	Předsíň	30+35,5		X	X	X	X	X	X	X			
25	1.19	WC ženy	30+35,5		X	X	X	X	X	X	X	X	X	X
26	1.20	WC muži	30+35,5		X	X	X	X	X	X	X	X	X	X
27	1.21	Odbor kanceláře tajemníka - sklad čisticích prostředků	30+35,5		X				X					
28	1.22	Odbor kanceláře tajemníka - sklad kancelářských potřeb	30+35,5		X				X					
29	1.23	Předsíň	30+35,5		X	X	X	X	X	X	X			
30	1.24	Odbor správy majetku města - dílna údržby	30+35,5		X	X	X	X						
31	2.01A	Odbor kanceláře tajemníka - sekretariát	30+35,5		X	X	X	X	X	X	X			
32	2.01B	Odbor kanceláře tajemníka - sekretariát	30+35,5		X	X	X	X	X	X	X			
33	2.02A	Kancelář místostarosty	30+35,5		X	X	X	X	X	X	X			
34	2.02B	Kancelář místostarosty	30+35,5		X	X	X	X	X	X	X			
35	2.03A	Zasedací místnost	EloLegic		X	X	X	X	X	X	X	X		
36	2.03B	Zasedací místnost	30+35,5		X	X	X	X	X	X	X	X		
37	2.04	Odbor kanceláře tajemníka - tisková mluvčí	30+35,5		X	X	X	X				X		
38	2.05A	Kancelář starosty	30+35,5		X	X	X	X	X	X	X			
39	2.05B	Kancelář starosty	30+35,5		X	X	X	X	X	X	X			
40	2.06A	Odbor kanceláře tajemníka - sekretariát	30+35,5		X	X	X	X	X	X	X			

Obr. 31 Výseč tabulky přidělených identifikátorů a práv přístupu konkrétním osobám

6.2.3 Údaje o cenách pro systém GHK

V této části uvedu orientační cenové údaje. Uváděné ceny jsou bez DPH a jsou pouze orientační a finální cena se může samozřejmě lišit. Použila jsem ceny dle nabídek jednotlivých společností, které se touto problematikou zabývají. Ceníky produktů jsou volně k dispozici na webových stránkách společností.

Tab. 10 Orientační cena systému GHK pro daný objekt

	Materiál	Počet (ks)	Cena za kus (Kč)	Cena celkem (Kč)
1.	Cylindrická vložka 30+35,5 mm	103	2 170	223 510
2.	Klíč k cylindrické vložce s elektr. identifikátorem	75	450	33 750
3.	Klíč GHK s elektronickým identifikátorem	1	1 100	1 100
4.	Elektromechanická vložka (EloLegic)	11	8 000	88 000
5.	Programovací zařízení k systému	1	22 100	22 100
6.	Software	1	15 000	15 000
	Cena celkem			383 460
	Předpokládaná sleva při odebraném množství	25%		
	Cena celkem po slevě			**287 595**

6.3 Kamerový systém

V celé budově není instalován žádný systém CCTV. Doporučila bych CCTV instalovat na všech vstupech do budovy a ve vybraných rizikových částech objektu. Data z CCTV budou směrována na centrum dohledové kontroly, které bude soustředěno v prostorách městské policie. Zálohovací zařízení zajistí možnost zpětného dohledání potřebných údajů ze záznamu.

Tab. 11 Průběh záznamu kamer u jednotlivých režimů

Nastavení kamer	
Režim RÁNO	kontinuální záznam
Režim DEN	
Režim NOC	záznam při změně obrazu

Provoz CCTV v areálu objektu musí zajistit soulad se zákonem č. 101/2000 Sb. O ochraně osobních údajů. Z hlediska tohoto zákona je nutné v budově rozmístit štítky s uvedením, že je objekt střežen kamerovým systémem.

Obr. 32 Návrh rozmístění kamer v 1. nadzemním podlaží

Obr. 33 Návrh rozmístění kamer v 2. nadzemním podlaží

V budově místní samosprávy budou v systému CCTV použity černobílé kamery s přísvitem pro noční vidění. Kamery mají vysokou citlivost i rozlišení, které je lepší než u kamer barevných. Napájení je zajištěno z externích zdrojů. Kamery jsou instalované na zdech pomocí držáků. Kamera umístěná na nádvoří je otočná, ostatní jsou pevně nastaveny na střežený prostor. Videosignály z kamer jsou přenášeny po koaxiálním kabelu.

U vybraných kamer je možné zahájit nahrávání pomocí detektoru pohybu. V tomto případě pomocí tzv. videodetektoru pohybu. Tato funkce elektronicky sleduje daný prostor, vymezenou oblast záběru kamery (okna, dveře, chodbu) a v případě změny obrazu, výše uvedeném detekování pohybu, se ve sledované oblasti automaticky spustí nahrávání. Výhoda této funkce je v tom, že šetří záznamovou kapacitu a v neposlední řadě také usnadňuje vyhledávání v pořízeném záznamu.

Tab. 12 Návrh kamer pro požadované prostory

Umístění	Nadzemní podlaží	Číslo prostoru	Minimální požadavky na kameru	Náhled	Orientační cena	Výrobce a typ kamery
Hlavní vchod	první	1.01	černobílá s přísvitem		3 700 Kč	Provision I4-370CSVF
Boční vchod	první	1.03	černobílá s přísvitem			
Chodba s historickými hodinami a vstupy k vedení města	druhé	2.12	černobílá s přísvitem			
Nádvoří	venkovní prostor	1.04	DOME kamera s přísvitem, vodotěsná, antivandal		4 200 Kč	Hikvision DS-2CC5281P-VP

Z příslušenství to budou dále držáky kamer (cca 150 Kč), kryty kamer (cca 1 200 Kč), ovládací klávesnice k DOME kameře (cca 9 500 Kč)

Zcela jistě není třeba zvlášť zdůrazňovat, že instalace veškerých technologií musí proběhnout podle návodů a pokynu výrobců. Vzhledem k tomu, že se jedná o historickou budovu, je nutné veškeré zásahy provádět co nejcitlivěji.

6.4 Kritéria pro hodnocení dodavatelů

Pro potřeby návrhu přístupového systému do administrativní budovy je třeba stanovit kritéria pro hodnocení jednotlivých dodavatelů systému. Nabízené systémy budou hodnoceny podle normy STN EN 1303. Pro výběr nebudou závazná všechna ustanovení této normy, a to z důvodu ceny dodávaných systémů.

V případě uzamykacích systémů generálním hlavním musí dodavatel splnit tato kritéria (pozn. požadovaná hodnota je v tabulce vyznačena barevně):

Certifikované vložky s požadovanou třídou bezpečnosti:

a) **Životnost (trvanlivost)** - musí umožnit ovládání cylindrické vložky novým originálním klíčem s krouticím momentem nepřesahujícím 1,5 Nm (Newtonmetr) po provedení počtu zkušebních cyklů.

Tab. 13 Životnosti vložek podle třídy bezpečnosti

Třída bezpečnosti	Počet cyklů
Třída 4	25 000
Třída 5	50 000
Třída 6	100 000

b) **Minimální počet efektivních kombinací** - bezpečnost související s klíčem, minimální počet kombinací musí odpovídat údajům v tabulce níže.

Tab. 14 Počet kombinací podle třídy bezpečnosti

Třída bezpečnosti	Minimální počet efektivních kombinací
Třída 1	100
Třída 2	300
Třída 3	15 000
Třída 4	30 000
Třída 5	30 000
Třída 6	100 000

c) **Odolnost proti napadení odvrtáním** - zub cylindrické vložky se nesmí po skončení zkoušky otočit bez příslušného klíče, použití krouticího momentu maximálně 5 Nm.

Tab. 15 Odolnost proti napadení

Odolnost proti napadení	Max. čas odvrtání (min)	Celkový čas zkoušky (min)
Třída 0	x	x
Třída 1	3	5
Třída 2	5	10

Garantovaná ochrana klíče proti kopírování - klíč je chráněný patentem, tím pádem se nedá volně kopírovat, což je zárukou proti zneužití klíče, dodavatel uvádí, na kolik let garantuje tuto ochranu.
Online servis - výroba klíče bez nutnosti návštěvy klíčové služby, objednávku je možné uskutečnit například prostřednictvím e-mailu na základě znalosti kódu klíče.

V případě CCTV musí dodavatel splnit minimálně tato kritéria - noční vidění, rozlišení, odolné proti povětrnostním podmínkám, úhlové vidění kamery minimálně 90^{o}. Kamery musí splňovat normy platné pro použití v České republice ČSN EN 50132.

V případě bezpečnostních fólií musí dodavatel minimálně tato kritéria - homologované na území Evropské unie, čiré, aby bylo v pracovních prostorech dostatek denního světla.

Společné požadavky na všechny dodavatele:
Kvalita dodavatele - u dodavatele, resp. výrobce zjišťujeme, jak dlouho je na trhu - delší doba je určitou zárukou kvality (např. alespoň 10 let), případně vlastní zkušenosti s tímto dodavatelem, jeho spolehlivost.
Kvalita dodávaného zboží - musí být zajištěna kvalita dodaného zboží, aby zboží splňovat požadované parametry.
Kompatibilita - kompatibilita elektronických identifikátorů se stávajícím ACS.
Cenové podmínky - cena dodávaných komponent, množstevní slevy.
Dodací podmínky - doba od objednání systémů až po jeho instalaci.
Platební podmínky - způsob platby a doba splatnosti.
Záruka - jak dlouhou záruku dodavatel poskytuje, jaký je pozáruční servis.
Reference - reference na dodavatele od jiných subjektů mohou být také důležitým vodítkem pro výběr dodavatele.

Pro snadnější výběr dodavatele, který bude splňovat naše požadavky nejlépe, můžeme například použít některou z metod výběru dodavatelů.

6.4.1 Metoda prostého hodnocení podle pořadí

Při prostém hodnocení podle pořadí provádíme hodnocení podle jednotlivých kritérií u všech dodavatelů. Při hodnocení přiřazujeme k jednotlivým kritériím body 1 – 3 (1 - vynikající, 2 - neutrální, 3 - špatné). Získané bodové ohodnocení u jednotlivých dodavatelů sečteme. Nejlepší dodavatel je ten, který získá nejnižší počet bodů.

Tab. 16 Hodnocení dodavatelů

Kritérium	Dodavatel		
	A	B	C
Kvalita (%)	100	90	75
Servis (%)	90	100	90
Cena (Kč)	320	287	260
Spolehlivost (%)	100	100	90

Tab. 17 Přiřazení bodového hodnocení

Kritérium	Dodavatel		
	A	B	C
Kvalita (%)	1	2	3
Servis (%)	2	1	2
Cena (Kč)	3	2	1
Spolehlivost (%)	1	1	2
CELKEM	7	6	8
POŘADÍ	**2**	**1**	**3**

6.4.2 Metoda váhového hodnocení pořadí

U váhového hodnocení vycházíme z metody prostého hodnocení, kdy ke každému kritériu přiřadíme předem stanovou váhu tak, aby nám celkový součet vah dal 100 %. Vahami kritérií vynásobíme přiřazené bodové hodnocení. Přiřazené bodové hodnocení následně vynásobíme vahami jednotlivých kritérií. Získané součiny u dodavatelů sečteme a následně vybereme dodavatele s nejnižším součtem. Podle toho určíme konečné pořadí.

Tab. 18 Váhové hodnocení podle pořadí

Kritérium	Váha kritéria (%)	Dodavatel		
		A	B	C
Kvalita (%)	60	0,6	1,2	1,8
Servis (%)	20	0,4	0,2	0,4
Cena (Kč)	10	0,3	0,2	0,1
Spolehlivost (%)	10	0,1	0,1	0,2
CELKEM	100	1,4	1,7	2,5
POŘADÍ		**1**	**2**	**3**

Záleží pouze na nás, která kritéria si vybereme pro hodnocení. Obecně se dá říct, že jsou to ta, která jsou v dané záležitosti stěžejní. K ostatním požadavkům na dodavatele přihlížíme, ale nemají rozhodující význam.

6.5 Vyhodnocení přínosu

Přínos nového režimového opatření spočívá v tom, že bude lépe zabezpečen přístup osob do budovy jasnými přístupovými právy. Zvýšení celkového zabezpečení budovy bude dosaženo instalací CCTV. Tím dojde ke snížení rizika spojeného s průnikem neoprávněných osob do vyhrazených zón a celkově ke zvýšení odolnosti budovy proti narušitelům.

Výhoda systému Generálního hlavního klíče spočívá v tom, že uzamykací systém je přehledným a hospodárným řešením vstupů, kde každý majitel klíče může svým klíčem uzamknout jen ty dveře, na které má oprávnění. Tyto uzamykací systémy se mohou použít

v každé oblasti – od zabezpečení rodinných domů, přes velké průmyslové objekty až po budovy pro veřejnost s komplikovanou hierarchií vstupních oprávnění.

Přínos systému je tedy v celkovém řízení přístupových práv do jednotlivých částí budovy s jasně vymezenými pravomocemi:

- evidence vstupů a zamezení neoprávněných vstupů do objektu,
- zvýšení zabezpečení proti neoprávněnému vniknutí do objektu,
- nenáročný servis systému,
- zvýšení efektivity řízení přístupových pravomocí,
- časová úspora,
- ochrana klíčů proti nelegálnímu kopírování.

Mezi výhody mechatronického klíče patří především:

Flexibilita – díky kombinaci mechanické a elektronické kontroly na jednom médiu může být použito v rámci kombinovaného systému na pouze mechanických, elektronických anebo kombinovaných komponentech systému.

Jednoduchá organizace vstupů - jednoduchá správa a programování umožňuje rychle organizovat oprávnění vstupů v rámci systému podle aktuálních požadavků i s časovým omezením. Ztráta klíče již nepředstavuje žádný problém, protože ztracený klíč může být ze systému elektronicky vyřazen.

Paměť událostí - každé dveře, které jsou vybaveny transponderem, mají vlastní paměť událostí. Zpětně je možné zjistit historii vstupů, stejně tak i pokusy o neoprávněné vstupy.

Jednoduchá instalace - externí napájení (baterie) zaručuje nezávislost systému. Kabeláž a případné opracování dveří v tomto případě není nutné.

Pořizovací náklady systému GHK rozhodně nejsou zanedbatelné, ale jsou nižší než pořízení nového elektronického systému ACS. V řešeném případě se jedná o historickou budovu, ve které by byla instalace kabeláže náročná a v některých místech nepřípustná z hlediska památkové ochrany. Systém GHK nezatěžuje budovu žádnou kabeláží a nepotřebuje ani připojení do elektrické sítě. Elektromechanické vložky jsou napájeny z vlastních baterií s životností 2 roky. Mechanických generálním klíčem je možné řešit jakékoliv dveře opatřené cylindrickou vložkou. Z těchto důvodů byl zvolen tento způsob zabezpečení.

ZÁVĚR

Neustálý nárůst kriminality klade na ochranu majetku, lidí a informací stále větší požadavky. S koncentrací množství lidí na malých plochách se zvyšuje i míra nebezpečí. V technické praxi se v současnosti rozšiřují a uplatňují přístupové systémy, které umožňují autorizovaný přístup do objektů. Se systémy ACS se v běžném životě setkává ve větší či menší míře většina z nás.

Kontrola vstupu do objektu by měla být jedním ze základních prvků bezpečnostní politiky každé organizace. Důvodů k implementaci ACS je několik, ale tím hlavním je zcela jistě zabezpečení prostor před neoprávněným vstupem nepovolaných osob. Integrace ACS s dalšími elektronickými informačními systémy nám umožňuje rychlejší a efektivnější práci, pružnější plánování a lepší využití finančních i lidských zdrojů. Navíc umožňuje efektivní kontrolu a přehled nejen o aktuální přítomnosti a pohybu osob v prostorách budovy, ale zároveň zpětně nahlédnout do evidence přístupů jednotlivých zaměstnanců do zabezpečených místností.

Provázáním ACS s navrženým kamerovým systémem můžeme získat další, tedy vizuální, zdroj informací o osobách, které vstupují do chráněných prostor, případně i o těch, kterým byl přístup odepřen. Propojení ACS s docházkovým systémem je kompatibilní řešení, kterým získáme spolehlivé komplexní řešení. Využití výhod automatizované správy a uložení dat si v dnešní době uvědomuje naprostá většina společností i firem, a proto po ní roste poptávka. Na trzích České republiky, stejně tak jako na zahraničním trhu, je celá řada společností, které nabízejí a poskytují přístupové systémy různého zaměření a rozsahu, jen je zapotřebí vybrat ten nejvhodnější pro daný objekt. Z počátku vyšší investice vynaložená na pořízení ACS se s postupem času mnohonásobně vrátí nejen ušetřeným časem, ale hlavně ušetřenými finančními prostředky, takže se vyplatí i menším společnostem.

Cílem mojí diplomové práce bylo navrhnout efektivní a plně funkční ACS pro konkrétní budovu místní samosprávy. Toto téma jsem si vybrala i z toho důvodu, že v této budově pracuji, tedy znám reálné podmínky a mohla jsem tak posoudit stav, výhody a nevýhody aktuálního řešení a svým návrhem přispět k úpravě a vylepšení systému. V tomto shledávám hlavní přínos a smysluplnost ve vypracování této práce.

V teoretické části jsem zpracovala problematiku o systému ACS a představila některé způsoby zabezpečení přístupu do objektů. Jedná se převážně o systémy využívající k identifikaci osob různé typy magnetických i čipových karet a v současné době velmi

moderní biometrické systémy. V praktické části jsem na základě získaných poznatků navrhla realizovatelné řešení ACS, který se i s rozšiřujícími systémy jeví pro daný objekt jako nejvhodnější. Součástí návrhu je vypracování organizačního schématu a nových režimových opatření. Tomu všemu předcházela analýza stávajícího systému, ze které vyplynula její pozitiva i negativa. Na základě zjištěných potřeb jsem následně stanovila kritéria pro hodnocení dodavatelů a uvedla přínos z navržených řešení.

Směr, kterým se bude problematika ACS v blízké budoucnosti ubírat, není lehké předpovědět. Nicméně z důvodu neustálého vývoje novějších technologií v oboru informatiky, hardware, software, ale také s nárůstem kriminality se budou systémy neustále vylepšovat, ale tím zároveň budou méně komfortní pro uživatele. Obecně platí nepřímá úměra, čím vyšší bezpečnost, tím nižší komfort pro uživatele. Tomuto se však do budoucna nevyhneme, neboť se vždy najdou útočníci, kteří budou chtít současný systém překonat. Proto je potřeba tyto technologie stále modernizovat a zdokonalovat.

CONCLUSION

We pay more and more attention to protection of our properties, people and information as there has been continuous increase in crime recently. The fact, that there is greater concentration of people in small areas, also increases the danger. There are access control systems known and used in engineering practice that allow authorized access into properties. Most of us have come across the ACS systems.

Checking the entrance to the building should be one of the key elements of each organization security policy. There are several reasons to implement ACS. However, the main reason is certainly the protection of the premises against unauthorized access by unauthorized persons. Integration of ACS with other electronic information systems allows us to work faster and more efficiently, to have more flexible scheduling and better utilization of financial and human resources. Furthermore, it provides efficient checks and overview of actual presence and movement of employees within the building, but it also allows you to re-look into the records for individual employees to enter the secure areas.

If we connect the ACS with the proposed camera system we can get another source of information, a visual one, about people who enter the protected area or the ones whose access to the premises is denied. Linking the ACS with the attendance system is a compatible solution, thanks to which we will obtain a fully integrated solution. The vast majority of companies do understand the importance of what advantage the automated management and data storage have. Therefore the demand is increasing. There are many companies that offer and provide access systems of different specification in the Czech Republic market as well as within the foreign markets. It is only necessary to choose the most appropriate one for a certain object. Initially, higher investment on purchase of the ACS will be paid off greatly not only by saved time but also by saved up funds. So it is attractive for smaller companies too.

The object of my assignment was to design an efficient and fully functional ACS for a specific building of local authority. I have also chosen this topic because I work in such building. Therefore I know real conditions and I could have evaluated the situation, advantages and disadvantages of the present solution. Furthermore, I hope that my proposal can contribute to modify and improve the system. This is the main asset and relevance of writing my assignment.

In the theoretical part I have worked out the issue of the ACS and I have introduced some methods about how to protect the access into premises. These are mainly systems that use different types of magnetic and chip cards for the identification of persons as well as biometric systems which are very modern these days. In the practical part I have proposed a solution of ACS based on the gained experiences which seems to be the most suitable for given premises also in terms of expanding systems. A part of my proposal is a design of a new organizational chart and a new regime policy. First of all, I have carried out an analysis of present system which showed its positives and negatives. Based on the identified needs I have set out the criteria for evaluation of suppliers and I have stated the benefits of the proposed solution.

It is not easy to predict which way the ACS will head in the near future. However, due to the continuous development of newer technologies in the field of computer science, hardware, software, but also with an increase in crime, the systems will constantly improve. On the other hand, they will be less comfortable for users. Generally we can say that the inverse relationship applies: the higher security, the less comfort for users. Unfortunately, we will not be able to avoid this in the future because there are always attackers willing to win over the present system. Therefore it is necessary to keep updating and improving such technologies.

SEZNAM POUŽITÉ LITERATURY

[1] ČANDÍK, Marek. *Objektová bezpečnost II.* 1. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004, 100 s. ISBN 80-731-8217-3.

[2] ČERNÝ, Josef, IVANKA, Ján a kol. *Systemizace bezpečnostního průmyslu I.* 1. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 2005, 134 s. ISBN 80-7318-310-2.

[3] ČSN EN 50133. Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011. Třídicí znak 334593.

[4] FERRARI, Elena. *Access Control in Data Management Systems*. San Rafael: Morgan, 2010, 423 s. ISBN 978-160-8453-757.

[5] KŘEČEK, Stanislav a kol. *Příručka zabezpečovací techniky*. 2. vyd. Blatná: Blatenská tiskárna, 2003, 351 s. ISBN 80-902938-2-4.

[6] LAUCKÝ, Vladimír. Technologie komerční bezpečnosti I. 1. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 2003, 64 s. ISBN 80-7318-119-3.

[7] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti I.* 3. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010, 81 s. ISBN 978-80-7318-889-4.

[8] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti II.* 2. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007, 123 s. ISBN 978-80-7318-631-9.

[9] LUKÁŠ, Luděk a kol. *Bezpečnostní technologie, systémy a management I.* 1. vyd. Zlín: Verbum, 2011, 316 s. ISBN 978-80-87500-05-7.

[10] NORMAN, Thomas L. *Electronic Access Control*. Waltham, MA: Butterworth-Heinemann, 2011, 423 s. ISBN 978-012-3820-280.

[11] ČSN EN 1303. Stavební kování – Cylindrické vložky pro zámky – Požadavky a zkušební metody. Praha: Český normalizační institut, 2005. Třídicí znak 165191.

[12] ŠENOVSKÝ, Michail, BALOG, Karel. Integrální bezpečnost. 1. vyd. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2009, 104 s. ISBN 978-80-7385-076-0.

[13] UHLÁŘ, Jan. *Technická ochrana objektů II. díl – Elektrické zabezpečovací systémy II*. 1. vyd. Praha: Policejní akademie ČR, 2005, 229 s. ISBN 80-7251-189-0.

[14] UHLÁŘ, Jan. *Technická ochrana objektů III. díl - Ostatní zabezpečovací systémy*. 1. vyd. Praha: Policejní akademie ČR, 2006, 246 s. ISBN 80-7251-235-8.

Internetové zdroje:

[15] Aktion [online]. 2013 [cit. 2013-05-03]. *Letecký snímek budovy*. Dostupné z WWW: http://www.aktion.cz/cs/sluzby-a-reseni/dochazkovy-system.html.

[16] Action One [online]. 2013 [cit. 2013-02-25]. *Docházkové terminály*. Dostupné z WWW: http://www.dochazkaonline.cz/dochazka/dochazkove-terminaly.html.

[17] Computer Word [online]. 2013 [cit. 2013-01-27]. Biometrické metody autentizace jsou výhodné. Dostupné z WWW:http://computerworld.cz/ securityworld/biometricke-metody-autentizace-jsou-vyhodne-49388.

[18] Kaba [online]. 2013 [cit. 2013-02-27]. *Klíč s identifikátorem EloLegic*. Dostupné z WWW: http://www.kaba.com/access-control/en/Products-Solutions/Electronic-Access-Control-standalone-systems/81174/kaba-elolegic.html

[19] Mapy CZ [online]. 2013 [cit. 2013-03-27]. *Letecký snímek budovy.* Dostupné z WWW: http://www.mapy.cz/.

[20] Saitech [online]. 2013 [cit. 2013-05-05]. *Zábranová zařízení*. Dostupné z WWW: http://www.saitech.cz/produkty/zabranova-zarizeni.

[21] Security magazín [online]. 2013 [cit. 2012-12-17]. *Bezpečnost z hlediska potřeb*. Dostupné z WWW: http://www.securitymagazin.cz/novinky/kategorie-odborne-clanky/soucasne-trendy.html

[22] Technopark [online]. 2013 [cit. 2013-03-12]. *Automatická závora*. Dostupné z WWW: http://www.technopark.cz/wil4-automaticka-zavora-delka-ramene-4m.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

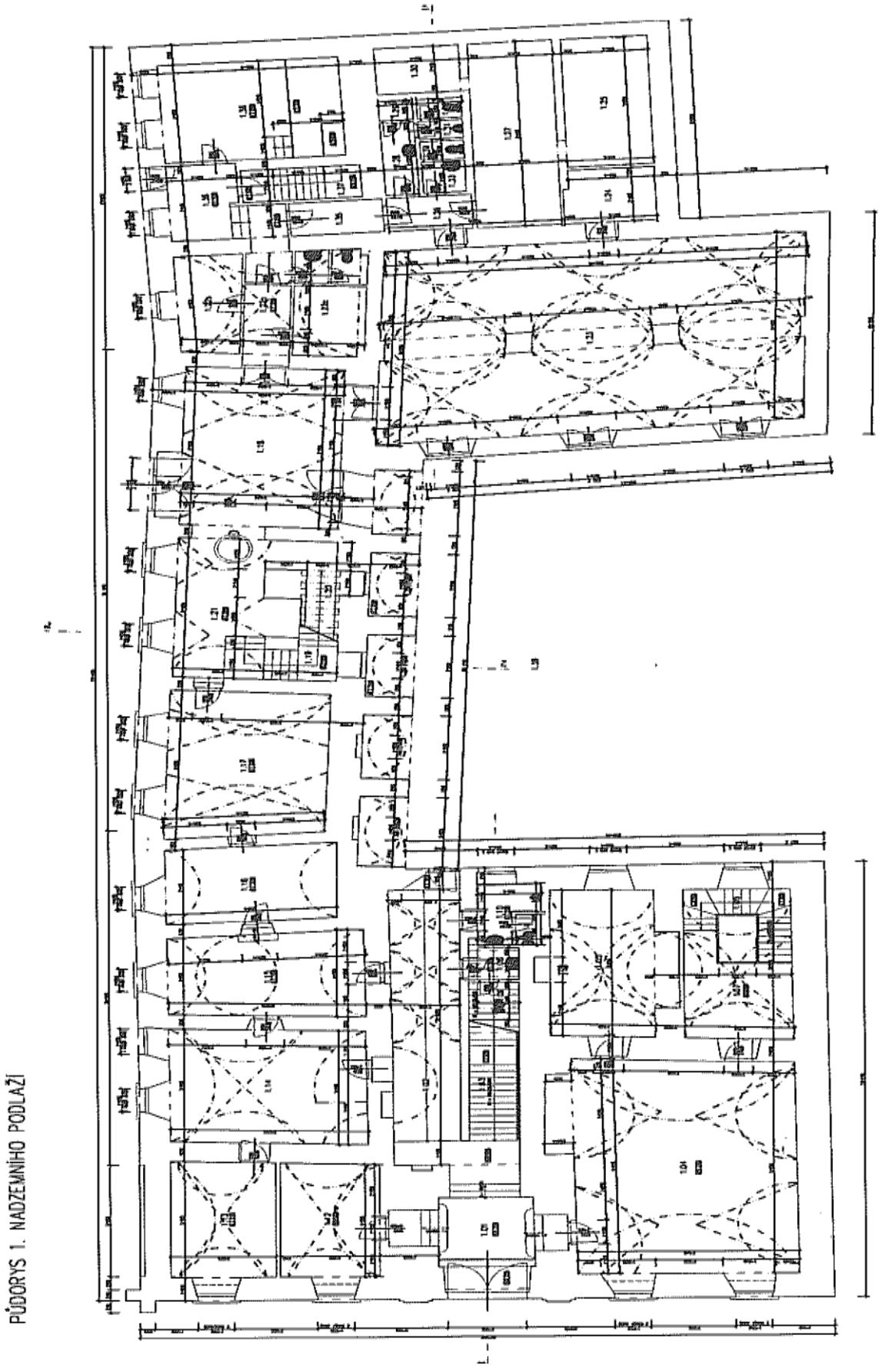
ACS	Access Control System (Přístupový systém)
APAS	Výstupní ovládací prvky a senzory místa přístupu
CCD	Charge Coupled Device (Zařízení pro snímání obrazové informace)
CCTV	Closed Circuit Television (Uzavřený televizní okruh)
CEN/TC	Technická komise evropských a mezinárodních normalizačních organizací
CENELEC	Evropský výbor pro normalizaci v elektrotechnice
ČSN	Česká státní norma
DNA	Deoxyribonukleová kyselina
DS	Docházkový systém
EMC	Electromagnetic Compatibility (Elektromagnetická kompatibilita)
EN	Evropská norma
EPS	Elektronický požární systém
GHK	Generální hlavní klíč
GHz	GigaHertz (Jednotka kmitočtu)
IEC	Mezinárodní výbor pro elektrotechniku
IR	Infrared Radiation (Infračervené záření)
MHz	MegaHertz (Jednotka kmitočtu)
NBÚ	Národní bezpečnostní úřad
Nm	Newtonmetr
PC	Personal Computer (Osobní počítač)
PIR	Passive Infrared (Pasivní infračervený senzor)
DPPC	Dohledové a poplachové přijímací centrum
PZTS	Poplachový a zabezpečovací tísňový systém
RF	Radiofrekvenční
RFID	Radio Frequency Identification (Radiofrekvenční identifikace)
RO	Režimová opatření
SK	Skupinový klíč
SKV	Systém kontroly vstupů
STN	Slovenská státní norma
V	Volt
VK	Vlastní klíč

SEZNAM OBRÁZKŮ

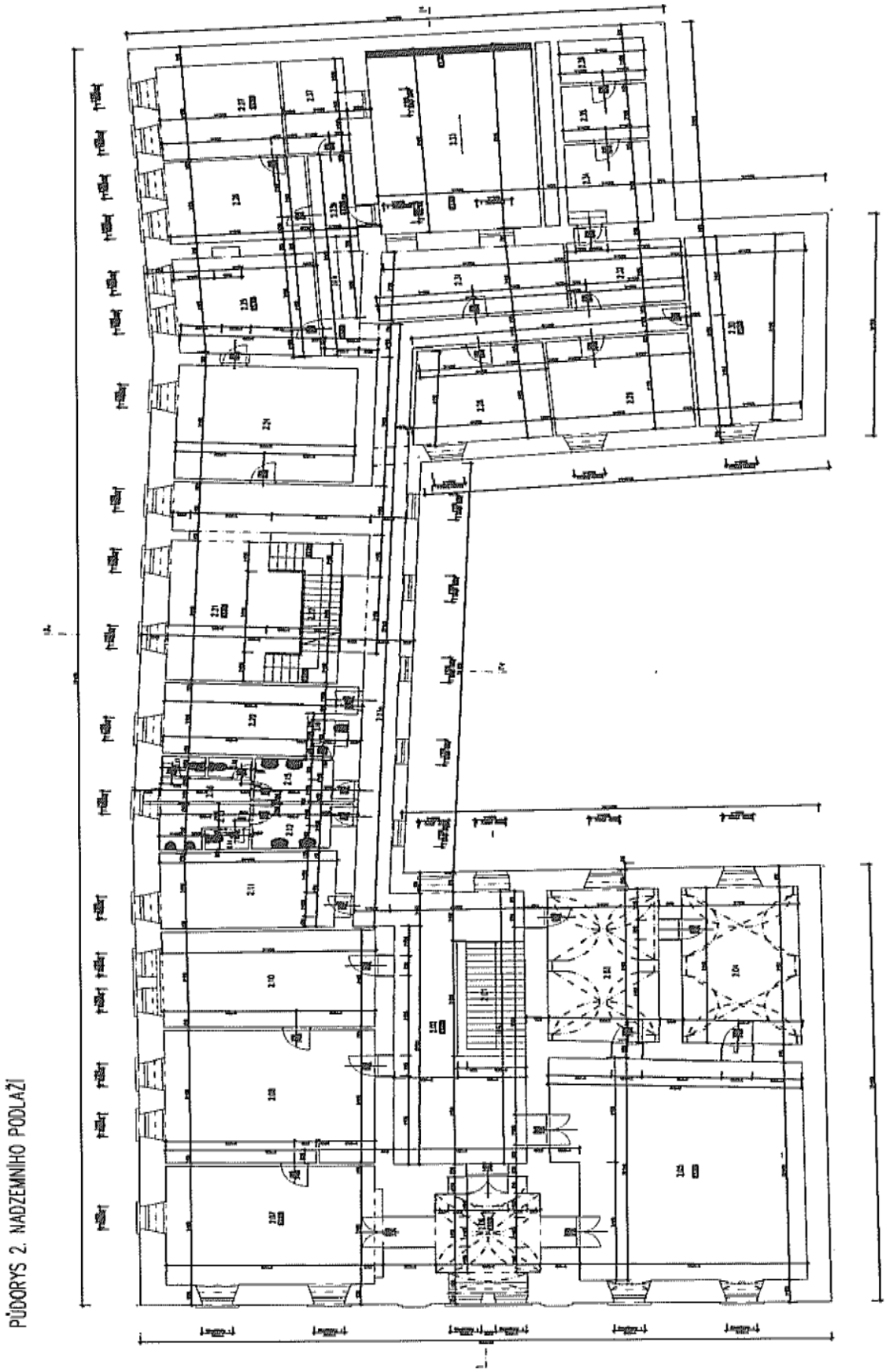
SEZNAM TABULEK

SEZNAM PŘÍLOH

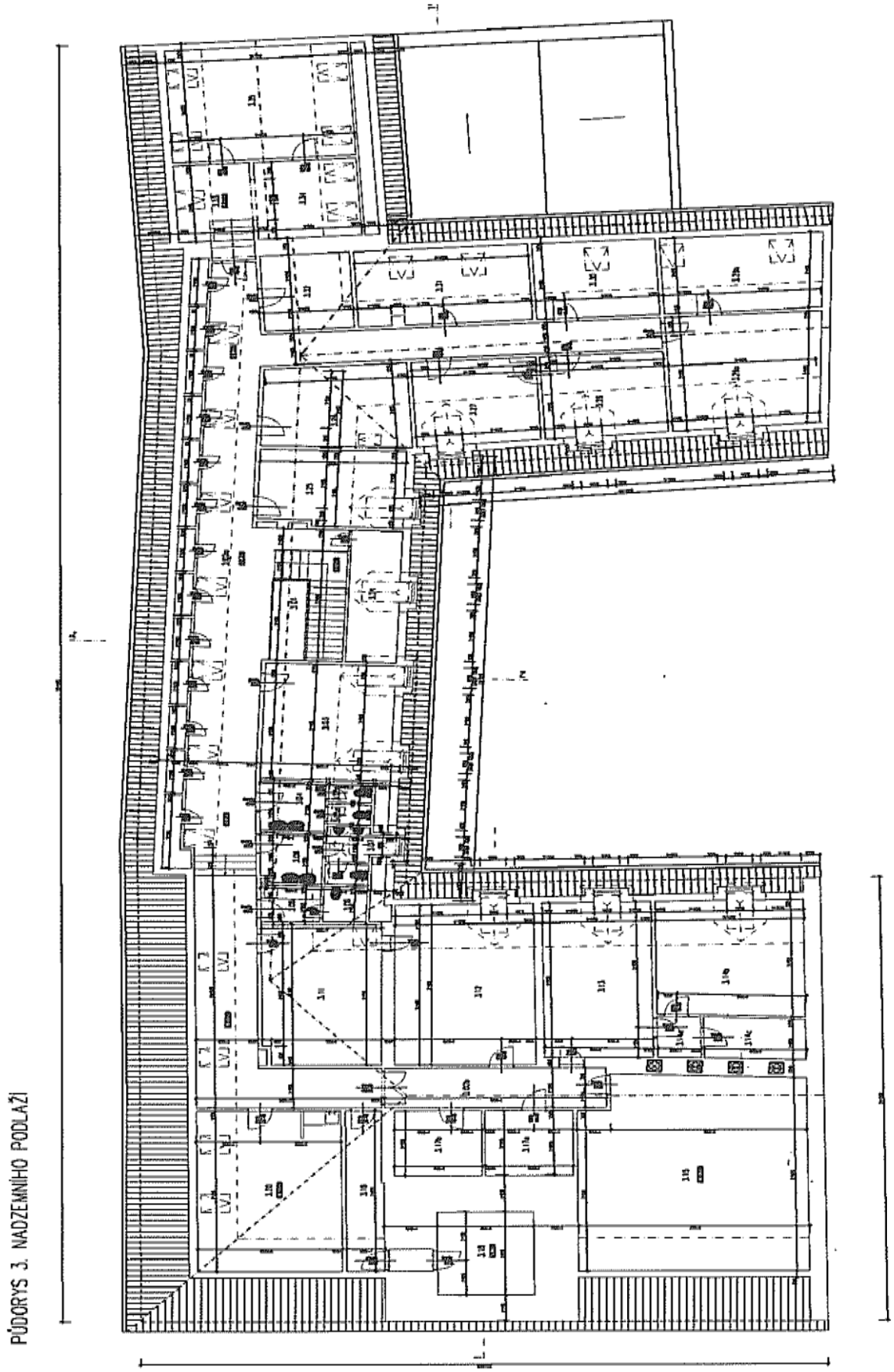
PŘÍLOHA P I: PŮDORYS 1. NADZEMNÍHO PODLAŽÍ



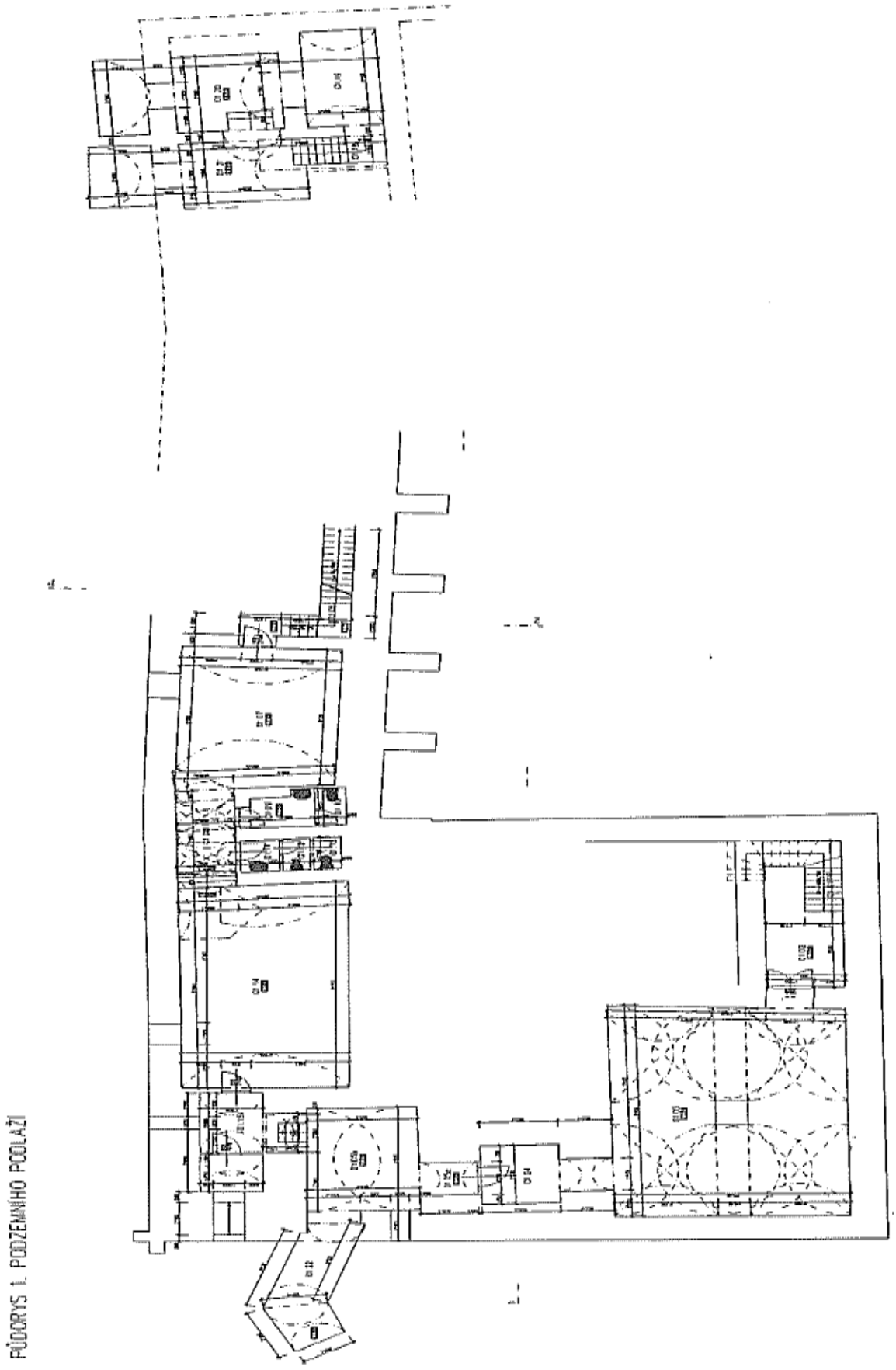
PŘÍLOHA P II: PŮDORYS 2. NADZEMNÍHO PODLAŽÍ



PŘÍLOHA P III: PŮDORYS 3. NADZEMNÍHO PODLAŽÍ



PŘÍLOHA P IV: PŮDORYS 1. PODZEMNÍHO PODLAŽÍ



PŘÍLOHA P V: PŘIDĚLENÍ IDENTIFIKÁTORŮ (KLÍČŮ) A PŘÍSTUPOVÝCH PR ÁV SYSTÉMU KONKRÉTNÍM OSOBÁM