Systém bezpečnosti informací v SW společnosti

System of information security SW company

Bc. Dagmar Kučová

Diplomová práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Dagmar KUČOVÁ**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Systém bezpečnosti informací v SW společnosti**

Zásady pro vypracování:

1. **Popište základní problematiku bezpečnosti informačních a komunikačních technologií.**
2. **Popište způsoby řešení zabezpečení administrativních budov proti externím i interním hrozbám, uveďte příklady z praxe.**
3. **Popište systém managementu bezpečnosti informací.**
4. **Navrhněte řešení bezpečnosti informačních a komunikačních technologií pro SW společnost s důrazem na vnitřní bezpečnost.**
5. **Navrhněte opatření, která povedou ke zvýšení bezpečnosti, růstu a konkurenceschopnosti společnosti.**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **EN ISO 9001:2000, Quality management systéme -- Requirements (Systémy managementu jakosti -- Požadavky)**
2. **ISO/IEC 13335-1:2004, Information technology -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management (Informační technologie -- Směrnice pro řízení bezpečnosti IT -- Část 1: Pojetí a modely bezpečnosti IT.)**
3. **ISO/IEC TR 13335-3:1998, Information technology -- Guidelines for the Management of IT security -- Part 3: Techniques for the management of IT security. (Informační technologie -- Směrnice pro řízení bezpečnosti IT -- Část 3: techniky pro řízení bezpečnosti IT.)**
4. **ISO/IEC TR 13335-4:2000, Information technology -- Guidelines for the Management of IT security -- Part 4: Selection of safeguards. (Informační technologie -- Směrnice pro řízení bezpečnosti IT -- Část 4: Výběr ochranných opatření.)**
5. **ISO 19011:2002 Guidelines for duality and / or environmental management systéme auditing (Směrnice pro auditování systému managementu jakosti a / nebo systému environmentálního managementu)**

Vedoucí diplomové práce:	**Ing. Ján Ivanka** Ústav bezpečnostního inženýrství
Datum zadání diplomové práce:	**19. února 2010**
Termín odevzdání diplomové práce:	**7. června 2010**

Ve Zlíně dne 19. února 2010

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práce se zabývá bezpečností informačních a komunikačních technologií a možnými způsoby zabezpečení administrativních budov. Práce je rozdělena na tři obecné části, ve kterých popisuji bezpečnost informačních a komunikačních technologií, systém managementu bezpečnosti informačních systémů a způsoby zabezpečení administrativních budov proti vnitřním nebo vnějším útokům.
V praktické části je zpracovaný realizační projekt pro SW Společnost se zaměřením na vnitřní bezpečnost.

Klíčová slova:

bezpečnost ICT, bezpečnostní politika, normy a standardy bezpečnosti IT, management bezpečnosti informačních systémů, zabezpečení administrativní budovy.

ABSTRACT

This thesis deals with security of information and communication technologies and the possible methods for securing office buildings. The thesis is divided into three general parts, which describe the security of information and communication technology, system security management information systems and methods for securing office buildings against internal or external attacks.

The practical part is treated by the implementation project for software company focused on internal security.

Keywords:

ICT security, security policy, standards and standards for IT security, management information systems security, security administration building.

Děkuji UTB ve Zlíně, za možnost studia na fakultě aplikované informatiky.
Děkuji vedoucímu diplomové práce panu Ing. Jánu Ivankovi.
Děkuji společnosti IDS Scheer, s.r.o., která mi umožnila studium při zaměstnání.
Děkuji společnosti Compactive, s.r.o., za možnost konzultace praktických řešení zabezpečení firem.
Děkuji manželovi a celé mojí rodině.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

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

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Vzhledem k neustálému vývoji informačních systémů ve společnostech, dochází k nárůstům citlivých dat a nasazování nových technologií pro jejich zpracování tím s sebou přináší zvýšené nároky na jejich zabezpečení. V současné době pronikají útočníci k cenným informacím zvenčí i zevnitř. Může tedy dojít k úniku informací, kdy jsou především ohroženy personální data, obchodní informace nebo know-how dané společnosti. Následky špatně zabezpečené organizace způsobenými ztrátami vedou k postupnému znevýhodnění na trhu a k jejímu celkovému oslabení.

V dnešní době musí být sledována ochrana budov podle nejnovějšího vývoje technologií zabezpečovacích systémů. Vlastník budovy musí umět pružně reagovat na tyto změny a zajistit inovaci systémů tak, aby bylo možné včas reagovat na případná rizika a tím eliminovat možné podmínky pro páchání trestné činnosti. Na otázky bezpečnosti je třeba nahlížet, jako na trvalý proces, který vyžaduje stálou údržbu a aktualizaci systémů s okamžitou reakcí na případné bezpečnostní incidenty.

Teoretická část diplomové práce je rozdělena na 3 kapitoly (1,2,3). V první a druhé kapitole jsou popsány základy bezpečnosti informačních a komunikačních technologií a management bezpečnosti informačních systémů, kde poukazuji na význam certifikované společnosti. Na závěr, tedy ve třetí části diplomové práce, jsou uvedeny možné způsoby zabezpečení administrativních budov pomocí vhodných systémů pro zajištění bezpečnosti uvnitř i vně budovy.

Praktická část diplomové práce je rozdělena na dvě základní kapitoly (4,5). V kapitole 4 je zpracovaný realizační projekt vhodného zabezpečení softwarové společnosti proti možným vnitřním nebo vnějším hrozbám. Vzhledem k vysokým nárokům na zabezpečení je projekt rozčleněn na tři hlavní části s detailním popisem konkrétních řešení podle způsobu zabezpečení. V první části je realizováno vnější zabezpečení na úrovni administrativní budovy. V druhé a třetí části je vnitřní zabezpečení společnosti, jednak na úrovni prvního patra administrativní budovy a podrobnějšího zabezpečení vnitřní bezpečnosti na úrovni systémů uvnitř společnosti. V kapitole 5 jsou uvedena opatření, která vedou k růstu společnosti, stabilní pozici na trhu a její konkurenceschopnosti.

V oblasti bezpečnosti informačních systémů se ve společnostech pracuje s velmi citlivými daty a veškeré informace a dokumentace týkající se tohoto tématu jsou důvěrné, tedy neveřejné, viz **Zákon 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti**. Z tohoto pohledu jsem pojala praktickou část diplomové práce, jako

realizační projekt, ve kterém jsem si nadefinovala neexistující společnost a inteligentní administrativní budovu. Navržené řešení zabezpečení je určené pro malou až středně velkou IT společnost. Řešení vnitřního zabezpečení společnosti na úrovni systémů, je konkrétně navrženo pro společnost Compative, s.r.o., která bude řešit vhodné zabezpečení uvnitř vlastní společnosti – viz. kapitola 4.5. na str. 76.

Realizační projekt je zaměřený na oblast zabezpečení budovy a ICT, nezohledňuje tedy ekonomickou nebo jinou stránku.

I. TEORETICKÁ ČÁST

1 BEZPEČNOST INFORMAČNÍCH A KOMUNIKAČNÍCH TECHNOLOGIÍ

Dříve jsme se mohli setkávat pouze s termínem IT - Informační technologie (dále jen „IT“). Pod tuto oblast bylo možné zahrnout veškerá elektronická zařízení, která byla schopna zpracovávat informace. Z tohoto hlediska se jednalo pouze o hardwarovou část. Postupem času došlo k vývoji technologií v oblasti IT. Jednotlivá zařízení spolu začala navzájem komunikovat a termín informační technologie byl rozšířený o nový prvek, konkrétně o komunikační technologii. V současné době se setkáváme s termínem ICT, tedy informační a komunikační technologie (dále jen „ICT“).

ICT slouží k výpočtům, zobrazování informací, jejich dalšímu zpracování a k dalšímu přenosu mezi uživateli. Můžeme je pro zjednodušení popsat, jako technologie, nástroje a postupy umožňující lidem komunikaci a práci s informacemi. Pod danou oblast můžeme zahrnout výpočetní techniku, mobilní komunikaci, síťové prostředky, zobrazovací techniku, prostředky pro sběr, přenos a ukládání dat.

ICT umožňují inovovat procesy i výrobky. Proto můžeme říci, že prostředky investované do výpočetních technologií přinášejí nárůst produktivity práce.

1.1 Obecně Bezpečnost ICT

Pod pojmem bezpečnost informačních technologií obvykle rozumíme ochranu odpovídajících informačních systémů a informací, které jsou v nich uchovávány, přenášeny a zpracovávány. Součástí takto obecně chápané bezpečnosti IT je i komunikační bezpečnost, jako ochrana informace přenášené mezi počítači, fyzická bezpečnost, tj. ochrana před přírodními hrozbami a fyzickými útočníky a personální bezpečnost, tedy ochrana před vnitřními útočníky.

Bezpečnost informačních systémů a komunikačních technologií, by měla být základem ve všech firmách a společnostech různých velikostí, které využívají IT systémy. Řešením bezpečnosti informačních systémů a informací musíme zajistit maximálně možnou a odpovídající ochranu před narušením, proti všem hrozbám, interního i externího původu a to s minimálními náklady.

Bezpečnosti IT zahrnuje prevenci a zmírnění takovýchto a podobných rizik. Informační bezpečnost je nepřetržitým úsilím o ochranu jednoho z nejcennějších aktiv každé společnosti a to informací. Informace uchovávané v systémech IT představují pro organizace kritické zdroje pro úspěšné plnění úkolů.

Systémy ICT musí splňovat svoji funkčnost a zároveň chránit informace před možnými riziky, kterými mohou být nežádoucí nebo neoprávněné šíření, změna či ztráta informací v organizaci.

1.2 Zabezpečení ICT

Jedním z hlavních aspektů, kterým se musí organizace zabývat, je důkladné zabezpečení informačních a komunikačních technologií. Základem je vytvoření takového prostředí, které zajistí informační bezpečnost a ochranu soukromí daného subjektu. Cílem je ochránit cenné informace, data i majetek, které je vlastnictvím organizace. Otázky bezpečnosti, tedy považuji za klíčové v rámci rozvoje informačních a komunikačních technologií. Jsou nezbytné pro růst kvality služeb zákazníkům. Narušení bezpečnosti může mít katastrofální pro všechny společnosti, organizace, podniky a jiné instituce.

Pro vytvoření lepší představy nyní uvedu příklady, jakým způsobem lze narušit bezpečnost organizace a naopak jakým vhodnými opatřeními zabezpečit ochranu organizace, jako celku.

K narušení bezpečnosti ICT dochází zejména odcizením, krádeží, zničením, špatnou manipulací a zacházením s hardwarem nebo softwarem, používáním informačního systému, který není autorizovaný a citlivá data a informace nejsou zabezpečena tak, aby k nim měla přístup pouze oprávněná osoba. Neznalostí a neinformovaností zaměstnanců.

Příklady vhodného zabezpečení ICT proti možným ztrátám v organizaci jsou:

- Zvýšením povědomí a odpovědnosti zaměstnanců
- Zabezpečení PC stanic, serverů a sítí
- Zabezpečený přenos dat a ochrana dat a komunikace
- Zálohování a archivaci dat
- Zálohování napájení
- Zálohování produktivních serverů a systémů
- Integrace fyzické, personální a ICT bezpečnosti

Z tohoto pohledu je zcela nezbytné, aby společnosti i organizace zabezpečovaly své informační systémy (dále jen „IS“) stejně, jako jiné investice do své činnosti.

1.3 Informační bezpečnost

V organizaci, společnosti nebo ve firmě musíme informace chránit proti narušení informační bezpečnosti, to znamená proti bezpečnostním incidentům. Bezpečnostní incidenty mohou být úmyslné nebo neúmyslné.

Úmyslné bezpečnostní incidenty, jsou vedené lidskými subjekty. Může se jednat buď o amatéry, nebo profesionály. Neúmyslné bezpečnostní incidenty mají různorodý původ, jako například výpadky elektrického napájení, síťové poruchy, poruchy softwaru a hardwaru, selhání lidského faktoru, jako nedostatečná kvalifikace uživatelů či nedodržování směrnic a manuálů. Také sem můžeme zařadit špatně navržený IS, který má za následek nedostatečnou kapacitu nebo výkon informačních technologií.

Porušení informační bezpečnosti a zákonů v organizaci má nemalé následky. Především se jedná o ztrátu důvěry svých zákazníků a klientů a také důvěryhodnosti celé společnosti. Vede k finančním problémům každé společnosti a dochází k ohrožení či dokonce ke ztrátě pozice na trhu a může vést až k samotnému zániku organizace.

Způsob, jakým můžeme chránit informace ve společnosti, nám určuje bezpečnostní politika. Základním konceptem je celková bezpečnostní politika ve společnosti. Informace můžeme chránit stanovením cílů a strategií, monitorováním provozu a následným vyhodnocením. Nástroje a prostředky realizace informační bezpečnosti jsou bezpečnostní funkce a bezpečnostní mechanismy.

1.4 Komunikační bezpečnost

Informační a komunikační technologie v dnešní době hrají nezastupitelnou roli v naší každodenní realitě, je nepostradatelnou součástí všech organizací, firem, institucí, ale i jednotlivce. Komunikace s okolním světem je jednou z nejzákladnějších potřeb každého z nás a již se stala součástí našeho života.

Bezpečná komunikační infrastruktura, která zajišťuje důvěrnost a neporušenost komunikace v různých prostředích, by neměla chybět v žádné společnosti využívající IT systémy.

Nejpřísnější bezpečnostní hlediska musí splňovat připojení vzdálené sítě i mobilního uživatele.

Pro dosažení bezpečnosti komunikačních technologií jsou nezbytná důkladná opatření, která povedou k bezpečné komunikaci v organizaci. Důraz se klade zejména na oblast zabezpečení přenosu dat a zabezpečení sítí, správou a dohledem. Nesmíme však

opomenout obranu proti možným útokům, jak vnitřních tak i vnějších. Opatření, která vedou k bezpečnosti komunikačních systémů, jsou zejména pomocí zajištění ověřování identity uživatelů, bezpečnostních auditů, testů zranitelnosti sítí a dalších.

Ve společnostech či organizacích je rozvoj komunikačních technologií vidět daleko více. Informační a komunikační technologie slouží pro uchovávání informací i pro jednodušší komunikaci. Můžeme tedy říci, že ICT podporuje a zefektivňuje obchodní aktivity téměř v jakékoliv oblasti podnikání.

1.4.1 Internetová komunikace

Citace [24]

„*Svět internetu nám nabízí synchronní a asynchronní způsoby komunikace. Synchronní komunikaci umožňují různé nástroje, např. chat, VoIP telefonie, případně Skype. Za asynchronní považujeme takové způsoby komunikace, při kterých není nutná okamžitá reakce, např. diskusní fóra a e-mail. Po internetu lze přenášet v digitální formě rozhlas i televizi, lze zajistit i další doplňkové služby v rozsahu podobném klasické telefonii a videotelefonii atd. apod*.“

Obr. 1 Telefonní ústředna [26]

1.4.2 Telekomunikační technika

Telekomunikační technika zahrnuje ucelená ICT komunikační řešení. Jedná se především o prostředky digitální nebo IP ústředen, call centra a sjednocené komunikace. Telefonní ústředna je zárukou spolehlivého spojení se zákazníky, klienty a obchodními partnery. Telefonní ústředny přináší vysoký komfort používání telefonu.

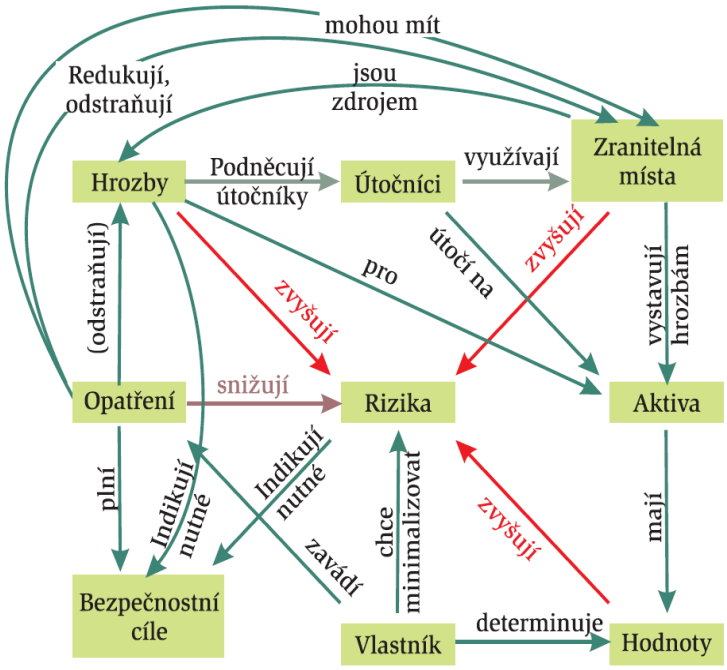
Pro soukromé účely nebo malé organizace jsou řešením menší zejména analogové ústředny, popřípadě i malé digitální ústředny. Pro malé a střední organizace, jako jsou státní instituce a úřady se nabízí řešení pomocí malých, avšak převážně středních digitálních ústředen. Pro velké organizace a nadnárodní společnosti, jako například společnosti s mnoha pobočkami po celém světě jsou řešením velké digitální a IP systémy a čistě softwarové řešení IP komunikace, které jsou nezávislé na hardwarové platformě.

1.5 Role bezpečnosti ICT

Bezpečnost ICT se stává v současnosti jednou ze základních vlastností informačních systémů. Zahrnuje prevenci a zmírnění možných rizik. Problémem zabezpečení vlastního informačního systému se zabývá pravděpodobně naprostá většina organizací rozdílného zaměření i velikosti.

Informace mají nezanedbatelnou hodnotu, proto musí být chráněny tak, aby k nim měly přístup jen oprávněné osoby. Nezbytná je také dostupnost informací a její ochrana proti vyzrazení. Bezpečný systém provádí určené funkce a chrání informace před riziky, jako je nežádoucí nebo neoprávněná šíření, ztráta či změna.

1.5.1 Obecný model bezpečnosti



Obr. 2 Obecný model bezpečnosti IS [6]

Zranitelné místo je slabé místo aktiva, v informačních systémech je dáno důsledkem chyb, zanedbáním nebo selháním v implementaci informačního systému nebo její analýze. Podstata zranitelného místa může být fyzická, například výpadkem proudu, pak přírodní, například požárem, nekontrolovatelným vstupem do budovy nebo důsledkem selhání lidského faktoru.

Zranitelnost je daná existencí zranitelných míst a potencionálních útočníků. Útočník může být vnější, ale čím dál častěji se vyskytuje i vnitřní útočník, který přímo působí ve společnosti či organizaci.

Vlastním nebo používám něco, co má pro mě nepominutelnou hodnotu je mým **aktivem**. Ztráta nebo snížení hodnoty mého aktiva mně způsobují škodu.

Útok je realizací hrozby a hrozba představuje možnost útoku. Ztráta nebo snížení hodnoty mého aktiva je důsledek útoku. Dopadem útoku je škoda způsobená realizovanou hrozbou. Útoky mohou být na hardware, software i data. Útočit lze přerušením, odposlechem, změnou (například změnou uložených dat), přidáním hodnoty (například podvržením nebo dodáním falešných dat). Útoky lze dále rozdělit na pasivní (odposlechem- zveřejnění obsahu zprávy, sledováním provozu,…) a aktivní (změnou, přerušením, přidáním hodnoty).

Hrozba, charakteristikou hrozby je její zdroj, motivace potencionálního útočníka, frekvence a kritičnost uplatnění hrozby. Hrozby můžeme rozdělit na objektivní (přírodní a fyzické, fyzikální, technické či logické) a subjektivní (neúmyslné a úmyslné), jedná se o hrozby plynoucí z lidského faktoru. Pravděpodobnost uplatnění hrozby chápeme, jako riziko.

Rizikem se rozumí možnost uplatnění něčeho, co má negativní vliv na moje aktiva nebo dosažení stanovených cílů. Pravděpodobnost a význam rizika se vyjadřujíce v pravděpodobnostních pojmech.

Stanovuji **bezpečnostní cíle,** které definují dosažení potřebné minimální hladiny rizik.

Ve společnostech IT je nutná prevence, abychom se vyvarovali před možnými útoky. Absolutní prevence útoků ovšem zajistitelná není, proto typická ochrana je založena na detekci útoků a následné obnově činnosti.

1.6 Základní cíle bezpečnosti IT

Informační systémy je nezbytné zabezpečovat. Jedná se o ochranu investic, neboť informace je zboží. Vedou nás k tomu právní nebo morální pravidla, činnost konkurence a zákonné úpravy pro ochranu dat.

V rámci bezpečnosti IT je bezpečnost dána zajištěním důvěryhodnosti, integrity a autenticity, dostupnosti a nepopíratelnosti.

- Důvěrnost

Důvěrnost má zásadní význam z hlediska ochrany dat. K údajům mají přístup pouze autorizované subjekty. Důvěrnost informačních systémů můžeme zabezpečit například udržováním bezpečných dat a zdrojů, šifrováním, udržováním dat v tajnosti či autorizací přístupů k datům, důvěrností procesů a komunikací.

- Integrita a autenticita

Integrita vede k zajištění správnosti a úplnosti informací. Aktiva, kterými jsou hardware, software a data, může modifikovat jen autorizované subjekty a původ informací lze ověřit. Autenticita, musí být zaručena ověřitelnost deklarovaného původu aktiva. Pro zajištění integrity softwaru je třeba používat kvalitní antivirové zabezpečení. Pro zajištění integrity dat používáme například digitálního podpisu, certifikátů a mnohé další.

- Dostupnost a nepopíratelnost

Dostupností rozumíme zajištění, že informace jsou pro oprávněné uživatele dostupné v případě potřeby. Aktiva jsou data nebo služby Ty jsou do určité doby dostupná, nedojde tedy k odmítnutí služby, kdy subjekt nedostane to, na co má právo.

Nepopíratelnost odesílání zprávy, přijetí zprávy, autorství dokumentu.

Bezpečný IS, je takový systém, který je zajištěn fyzicky, administrativně, technicky i logicky.

1.7 Bezpečnostní cíl, funkce a mechanismus

Informační systémy jsou v současnosti ohrožovány řadami hrozeb a každým dnem přibývají nové metody útoku. Cílem je snížit riziko lidské chyby, krádeže, podvodu nebo zneužití prostředků organizace či podniku. Uživatelé si musí být vědomi bezpečnostních hrozeb a otázek s nimi spjatých, musí se podílet na dodržování politiky bezpečnosti informací v průběhu své práce. Je třeba minimalizovat škody způsobené bezpečnostními incidenty a chybami, sledovat je a učit se z nich.

Bezpečnostní opatření musí účinnou formou implementovat vhodnými mechanismy.

V případě, že zabezpečujeme IS, musíme si nejprve stanovit bezpečnostní cíle a způsob jejich dosažení. Prostředkem použitým pro dosažení stanovených bezpečnostních cílů jsou bezpečnostní funkce IS, které mohou být administrativního, fyzického nebo logického typu, to znamená, že mohou být implementovány takovými mechanismy, jakými jsou administrativní akce, hardwarová zařízení, procedury, programy. Podle okamžiku uplatnění dělíme bezpečnostní funkce na preventivní odstraňující zranitelná místa, heuristické snižující riziko dané hrozbou, detekční a opravné minimalizující účinek útoku.
Podle způsobu implementace rozeznáváme bezpečnostní funkce:

- Softwarového charakteru, digitální podpis, zřizování účtů
- Administrativního a správního charakteru, školení osob, hesla, normy, vyhlášky
- Hardwarového charakteru, šifrovače, firewally, archivní pásky
- Fyzického charakteru, trezory, zámky, strážní, protipožární ochrana

1.8 Bezpečnostní politika

Bezpečnostní politika určuje způsob dosažení bezpečnostních cílů. Definuje, co se chrání proti čemu, stanovuje bezpečnostní cíle a uplatnění ochrany.
Bezpečnostní politika IT organizace obecně vymezuje, co vyžaduje ochranu, proti jakým hrozbám je ochrana budovaná a jak budeme chránit, to co vyžaduje ochranu.

1.8.1 Bezpečnostní politika IT organizace

Celková bezpečnostní politika stanovuje bezpečnostní infrastrukturu sítě, stanovuje citlivá aktiva, jejich klasifikaci, odpovědnosti za jejich stav. Určuje výběr bezpečnostních zásad a předpisů souvisejících se zabezpečením IT. Není závislá na konkrétní používané IT.
Systémová bezpečnostní politika určuje detailní normy, pravidla, praktiky, konkrétní definice správy, ochrany, distribuce citlivé informace a jiných IT zdrojů v rámci organizace. Specifikuje způsob implementace a použití bezpečnostních opatření zaručujících přiměřenou bezpečnost. Respektuje použité informační technologie.
Systémová bezpečnostní politika informačního systému stanovuje konkrétní cíle a opatření a použité mechanismy pro implementaci, definuje havarijní plán a plán činnosti po útoku.

- **Analýza rizik**

Analýza rizik je nejdůležitější částí bezpečnostní politiky. Výstupem jsou dokumenty, které obsahují výsledek analýzy, jedná se o popis systému, zjištění hrozeb a rizik, zjištěná

ranitelná místa, zjištěná úroveň stávajících bezpečnostních opatření, návrh bezpečnostních opatření snižujících rizika, kterým je IS vystaven.

- **Havarijní plán**

Určuje postup pro případ, že dojde k útoku, definuje, jak postupovat, aby se udržel chod organizace. Zahrnuje i plán činnosti po útoku a plán obnovy.

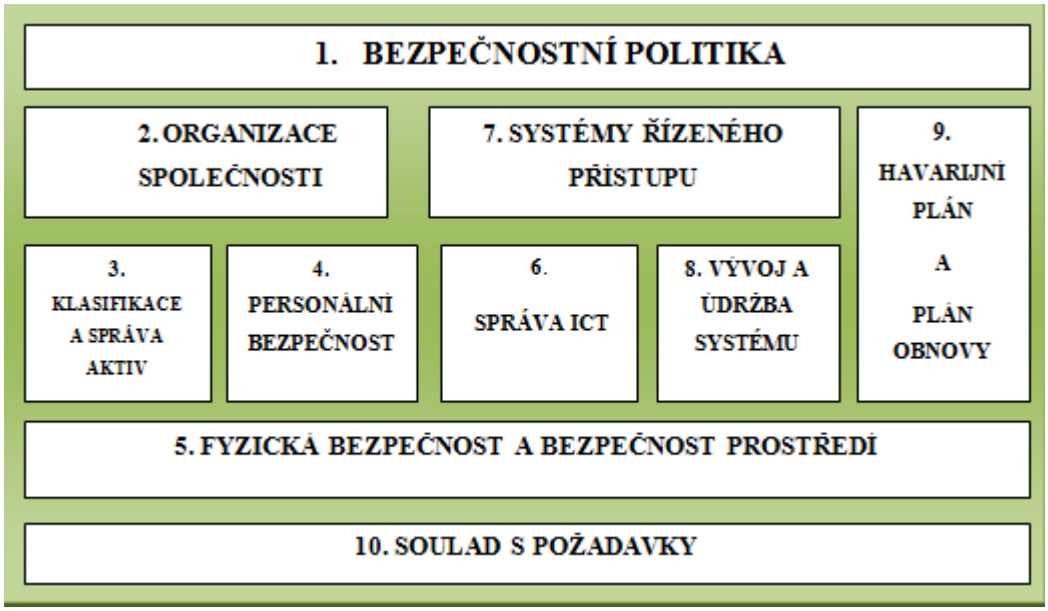
- **Bezpečnostní audit**

Bezpečnostní audit kontroluje, zda byli správně definované bezpečnostní postupy a bezpečnostní opatření. Kontroluje procedury, které následovaly po narušení bezpečnosti. Stanovuje důvod a zodpovědnost za narušení bezpečnosti.

- **Přínos a opatření**

Opatření přispívají ke snížení zranitelnosti organizace. V případě, že už dojde k incidentu je k dispozici náhradní řešení a podle zpracované metodiky se zjistí příčina a přijmou se účinná ochranná opatření. Organizace čím dál častěji požadují po svých partnerech důkazy, že se s jejich daty zachází bezpečně a nehrozí zneužití poskytnutých údajů.

Rozpoznat a definovat rizika můžeme přijetím adekvátních opatření pro zvýšení bezpečnosti. Například zlepšením organizační struktury. Správnou kombinací bezpečnostních opatření na všech úrovních systému lze minimalizovat riziko jejich napadení. Bezpečnost není jen záležitostí vybraných expertů ale všech pracovníků organizace. Bezpečnostní opatření pro ochranu informací můžou být implementovány do odpovídajících materiálů upravujících vnitřní chod firmy, jako je pracovní řád, interní směrnice, pracovní postupy, provozní předpisy, technická provozní dokumentace a další.



Obr. 3 Bezpečnostní politika

Postavení bezpečnostní politiky ve společnosti

1. Základním a strategickým dokumentem je bezpečnostní politika. Definuje základní koncepci ochrany informačních aktiv organizace. Cílem je zajištění řízení a podpory pro informační bezpečnost. Obsahuje pravidla, směrnice a praktiky, které rozhodují o tom, jak jsou aktiva včetně citlivých informací spravovány, chráněny a distribuovány uvnitř organizace a jejich systémů IT.
2. Ve společnosti či organizaci je nezbytné udržovat organizační a provozní pravidla. Politika informační bezpečnosti vymezuje cíle, oblasti, role a management.
3. Klasifikace a správa nám definuje, jak vhodně zajistit ochranu podnikových aktiv tak, aby informace měly požadovanou úroveň ochrany.
4. V oblasti personální bezpečnosti je cílem zvyšovat odbornost zaměstnanců a poskytnout jim patřičná školení na různých úrovních. Nezbytným prvkem ve společnosti je bezpečnostní informovanost.
5. Pomocí prostředků fyzické bezpečnosti musíme zabránit neautorizovaným přístupům, ztrátám nebo zneužívání aktiv a tím zajistit vnitřní i vnější bezpečnostní ochranu.
6. Správa ICT zajistí správnost a bezpečnost zařízení, která zpracovávají informace, zabrání ztrátám, modifikacím a zneužití informací při jejich výměně mezi organizacemi. Musí umět minimalizovat rizika systémových selhání a chránit integritu SW a informací.
7. Systémy řízeného přístupu, cílem je zabránit neautorizovaným přístupům k informačním systémům a počítačům a zajistit ochranu síťových služeb.
8. Vývoj a údržbu systému zajistíme zabudováním bezpečnostních prvků do operačních systémů, tím zabráníme možným ztrátám a zneužití uživatelských dat v programových aplikacích. Cílem je ochránit důvěrnost, autentičnost a integritu informací.
9. Havarijní plány a plán obnovy, cílem je zabránit přerušení podnikových aktivit po závažných selháních IS a po katastrofách. Zachování kontinuity byznysu, BCP - Business continuity plan.
10. Soulad s požadavky s již existující legislativou a jinými bezpečnostními normami a předpisy nám říkají, že cílem je vyvarovat se střetům s trestní nebo občanskou legislativou a zajistit soulad systémů s podnikovými bezpečnostními normami. Maximalizovat účinnost auditů systému a minimalizovat jejich rušivé dopady.

1.9 Normy a standardy používané v oblasti bezpečnosti informačních technologií

Bezpečnostní normy jsou důležitým prvkem informační bezpečnosti. V průmyslovém světě znamenají jednu ze zásadních cest předávání znalostí, snižování nákladů a umožnění vzájemné spolupráce a kompatibility produktů. Normy jsou dokumentované dohody, které určují pravidla, kritéria, definice, směrnice k zajištění správných a účelných postupů ve společnosti.

1.9.1 Nadnárodní, celosvětové standardizační organizace

Citace [32]

„Mezi nejvýznamnější mezinárodní organizace, které se zabývají vedle ostatní standardizační činnosti i standardizací bezpečnosti IT, patří

- *International Organization for Standardization (ISO)*
- *International Electrotechnical Comission (IEC)*
- *International Telecommunications Union (ITU) „*

  - International Organization for Standardization (ISO)

Posláním ISO je podporování rozvoje standardizačních a s tím spojených aktivit. Celosvětová federace národních standardizačních institucí z více než 140 zemí, byla založena od roku 1947.

1.9.2 Informační bezpečnost podle ISO/IEC

- ISO/IEC 27001

Information security management system – Requirements

- Požadavky na implementaci ISMS
- Požadavky na implementaci opatření podle ISO/IEC 27002
- Specifikuje, jak vybudovat systém, který posuzuje, implementuje, monitoruje a udržuje bezpečnostní systém organizace
- ISMS lze proti ISO/IEC 27001 certifikovat
- Základ pro třetí stranu provádějící audit ISMS

Zavedení ISMS

- Definování oblasti
- Provedení odhadu rizik (ISO/IEC 13335)

- Identifikace a hodnocení voleb pro správu rizik
- Určení bezpečnostních cílů a politiky
- Příprava dokumentů, seznam vybraných opatření
- Implementace a provozování ISMS
  - ISO/IEC 27002

Doporučení, jak navrhnout, implementovat, udržovat a vylepšovat správu informační bezpečnosti v organizaci. Návod pro budování bezpečného systému.

- ISO/IEC 27004

Míry efektivnosti implementace ISMS

- Jak je systém spravovaný, cíle, pravidla, role, procedury, audity
- Technické vlastnosti, jako výkon, komunikační vlastnosti a další
- Fyzické podmínky k provozu budovy, energie, řízení přístupu
- Vzdělanost a znalost personálu
  - ISO/IEC 13335
- Koncepty a modely tvořící základ pochopení IT bezpečnosti
- Techniky provádění analýzy rizik
  - ISO/IEC 15408

Kritéria pro hodnocení bezpečnosti IT. Norma uvádí obecná hodnotící kritéria, která by měl být schopen kupovaný anebo vyvíjený produkt splnit.

- 15408-1 Úvod a všeobecný model
- 15408-2 Bezpečnostní funkční požadavky
- 15408-3 Požadavky na záruku bezpečnosti

1.10 Shrnutí zabezpečení ICT

Význam informačních a komunikačních technologií stále stoupá. Vyvíjí se stálé nové technologie a systémy, které přispívají k efektivnější a bezpečnější práci a komunikaci. ICT jsou dnes součástí většiny našich aktivit a tím roste význam pro jejich každodenní použití. Proto je třeba klást veliký důraz na bezpečnost ICT a tím zabránit ztrátě či úniku informací, popřípadě zničení nebo odcizení majetku. Účinnou formou ochrany ICT v každé společnosti je zavedení systému řízení bezpečnosti informací ISMS.

2 MANAGEMENT BEZPEČNOSTI INFORMACÍ

Rozvoj počítačových technologií a informačních systémů přináší s sebou nezbytnost ochrany dat a zavedení účinného managementu bezpečnosti informací. Bezpečnost informačních technologií je vhodná pro kteroukoliv organizaci ať už ze státní sféry či podnikatelské sféry včetně institucí.

Management bezpečnosti informací je především určený pro organizace, které pracují s informacemi. Cílem je zamezit jejich ztrátě, odcizení nebo zneužití. Důraz je kladen zejména na ochranu osobních údajů, firemních údajů, dat od zákazníků a dodavatelů nebo možného vyzrazení know-how. Zahrnout sem můžeme tato klíčová odvětví, jako jsou banky, pojišťovny, veřejné instituce, jako například orgány státní správy, úřady nebo marketingové společnosti a průmyslové podniky, dále pak i zdravotní zařízení, školy, dopravce a e-organizace, a další organizace.

- **Bezpečnost informací**

Citace [3]

„Informační bezpečnost je s managementem organizace spojena dvěma vazbami. První je souvislost marketingová. Pokud organizace zvyšuje svou důvěryhodnost na trhu cestou certifikace svého systému managementu jakosti, musí očekávat také auditorský dotaz na úroveň zabezpečení informací. Druhou souvislostí je neoddělitelnost informace od řízení organizace i od podnikových procesů samotných. Informace je v tomto případě zdrojem, podobně, jako peníze nebo pracovníci. Nezajištěnost vlastních zdrojů ohrožuje produkci, tedy vstupy zákazníků a tím vede k růstu rizik pro organizaci samotnou a k lavinovitému šíření hrozeb do okolního komerčního prostředí“.

2.1 Certifikace systému managementu bezpečnosti informací

ISMS (Information Security Management System – systém managementu bezpečnosti informací), je částí celkového systému řízení procesů organizace, který dokumentuje, implementuje, přezkoumává, udržuje a zlepšuje proces bezpečnosti informací.

Cílem systému managementu bezpečnosti informací (dále jen ISMS“) je chránit informační aktiva organizace tak, aby nedošlo k jejich zneužití či ztrátě. Je uplatňován za účelem vyhodnocování možných rizik a k uplatnění řídicích mechanismů ve společnosti. ISMS může být zaveden pro organizační složku společnosti, nebo jeho část, případně může zahrnovat celou organizaci. Vede k zachování důvěrnosti, integrity a dostupnosti informací.

Zavedení ISMS je strategickým rozhodnutím vedení společnosti.

2.1.1 Výhody certifikovaného systému ISMS

Certifikovaný ISMS je posuzován externí nezávislou institucí, která uděluje značku i certifikát. Výhodou certifikované společnosti je zvýšení důvěryhodnosti pro různé skupiny, jako jsou klienti, autority, finanční ústavy, spolupracující organizace, kontinuální monitorování a zlepšování ochrany dat a bezpečnosti informací a konkurenční výhoda a také image organizace.

ISMS je zcela potřebný všude tam, kde se zpracovávají informace a data občanů. V dnešní době je to požadavek většiny moderních firem. Je nezbytný v oblasti outsourcingu a v oblasti zakázek pro státní správu a pro velké nadnárodní firmy.

Zejména jde o poskytnutí důvěry a především důkazu o tom, že jsou v organizaci uplatňovány důvěryhodné postupy v oblasti bezpečnosti IS.

2.2 Certifikace systému managementu bezpečnosti informací podle ČSN ISO/IEC 27001

Zavádění a certifikace systémů managementu bezpečnosti informací podle ISO/IEC 27001 je relativně mladá disciplína. Norma byla vydána v roce 2005 a od té doby zaznamenala rychlý vývoj. O zavedení certifikace mají především zájem ty organizace, které disponují velkými objemy důvěrných dat. Může se jednat o organizace z řad soukromých, ale i o státní sféru.

Mezinárodní norma ČSN ISO 27001 prosazuje přijetí procesního přístupu pro ustanovení, zavádění, provozování, monitorování, udržování a zlepšování ISMS v organizaci.

Certifikace dle ČSN ISO/IEC 27001 (dle mezinárodní normy zaměřené na ISMS), je aplikovatelná v jakékoliv organizaci a to ve všech oblastech výroby nebo poskytovaných služeb. Podle ní se hodnotí a posuzuje systém informační bezpečnosti. Systém managementu dle požadavků normy ISO 27001 je určen všem organizacím, které chtějí získat nejen konkurenční výhodu, ale které chtějí chránit svá informační aktiva a tím minimalizovat ztráty způsobené jejich únikem.

Jsou uplatněny stejné principy budování a zdokonalování ISMS postavené na základě PDCA cyklu.

2.2.1 Postup certifikace ISMS podle normy ČSN ISO 27001

- Schválení zlepšování ISMS
- Řízení a realizace nápravných/preventivních kroků
- Kontrola účinnosti aplikovaných protiopatření
- Přezkoumání ISMS vedením
- Řízení rizik
- Aplikace politiky ISMS, opatření, procesů a postupů
- Stanovení politiky, cílů, rozsahu působnosti ISMS
- Analýza rizik

V rámci certifikačního auditu se musí posuzovat systematický přístup založený na rozhodnutí vedení o míře přijatelnosti rizik. Musí se zohlednit způsob, jakým bude organizace se svými riziky nakládat. Vytvořit povědomí mezi zaměstnanci, do jaké míry má vliv každý zaměstnanec na své pozici na bezpečnost informací. Nezbytné je i posouzení technické a objektové bezpečnosti.

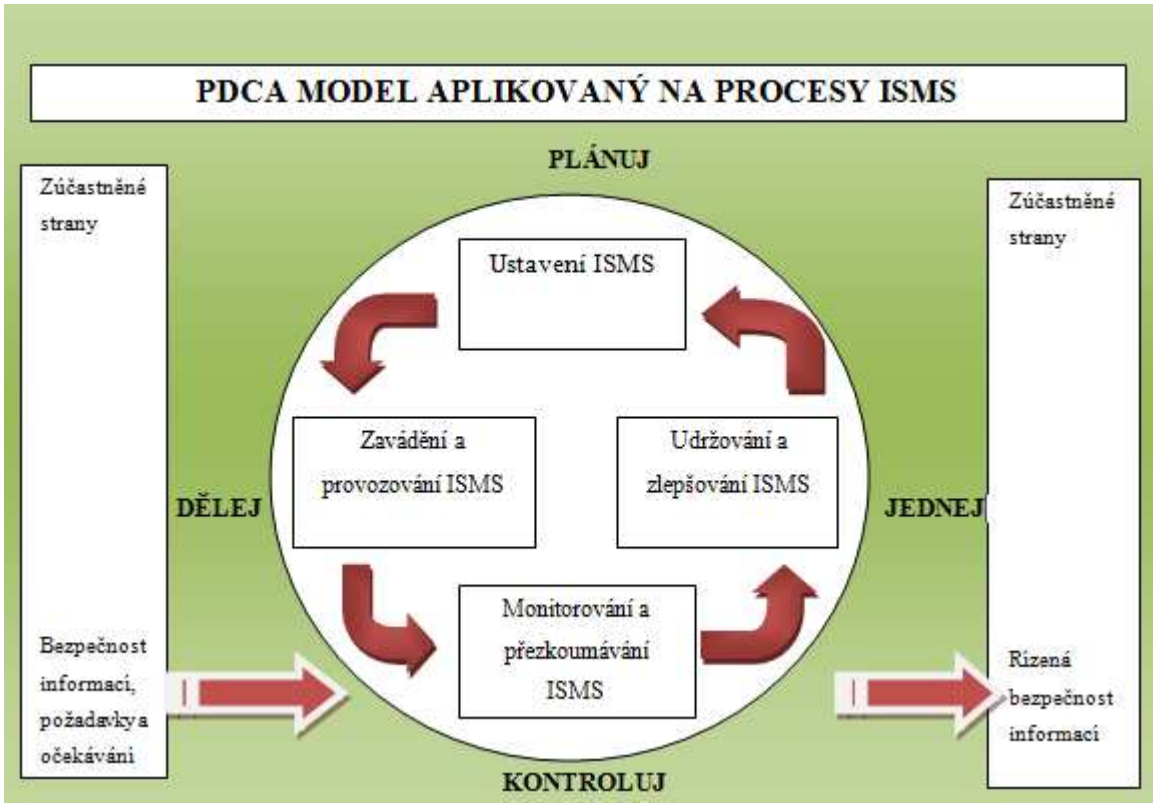
Přínosem certifikace podle ISO/IEC 2701 je soulad s legislativními předpisy, zajištění konkurenční výhody, jako je zlepšení image společnosti, plnění požadavků zákazníků a jiné. Dalším přínosem je snížení rizik souvisejících s únikem nebo ztrátou informací a úspory nákladů. Důležitým aspektem je i zvýšení povědomí pracovníků tím, že se jednoznačně vymezí odpovědnosti a pravomoci při nakládání s informacemi ve společnosti.

Mezinárodní norma ČSN ISO 27001 je navržena tak, aby organizaci umožnila propojit nebo integrovat ISMS s odpovídajícími požadavky systému managementu. Můžeme tedy o ni říci, že je kompatibilní.

2.3 Smyčka PDCA

Norma zavádí model, Plánuj-Dělej-Kontroluj-Jednej - Plan-Do-Check-Act, (dále jen „PDCA“), jako součást přístupu systému řízení k vývoji, implementaci a zdokonalování efektivnosti systému řízení bezpečnosti informací v organizaci. Smyčka PDCA představuje model, který je aplikovatelný na procesy ISMS. Cílem je pomoci zavést do organizací systémový přístup k bezpečnému zajištění firemních informací.

- **Klasický přístup systému řízení, představuje charakteristická smyčka PDCA.**



Obr. 4 PDCA model aplikovatelný na procesy ISMS [12]

- Plánuj

Vytvoření bezpečnostní politiky, plánů, cílů, procesů a procedur souvisejících s řízením rizik a zlepšováním bezpečnosti informací tak, aby poskytovaly výsledky v souladu s celkovou politikou a cíli organizace.

Musíme stanovit rozsah ISMS a politiky ISMS. Dále definovat přístup k posuzování a identifikaci rizik. Naplánovat postup identifikace a hodnocení podmínek pro ošetření rizik. Stanovit výběr bezpečnostních opatření a jejich cílů. Připravit dokument SOA (Statement of Applicability).

- Dělej

Zavedení a využívání bezpečnostní politiky, řízení, procesů a procedur zahrnuje formulace plánu k ošetření rizik, implementace plánu k ošetření rizik, implementace bezpečnostních opatření a implementace školení, budování povědomí, řízení činností a zdrojů. Implementace procedur pro detekci incidentů a reakce na incidenty.

- Kontroluj

Ověření úrovně, tam, kde je to možné, provádění procesu vůči bezpečnostní politice, cílům a praktické zkušenosti a oznámení výsledků řízení k posouzení. Kontrola zahrnuje

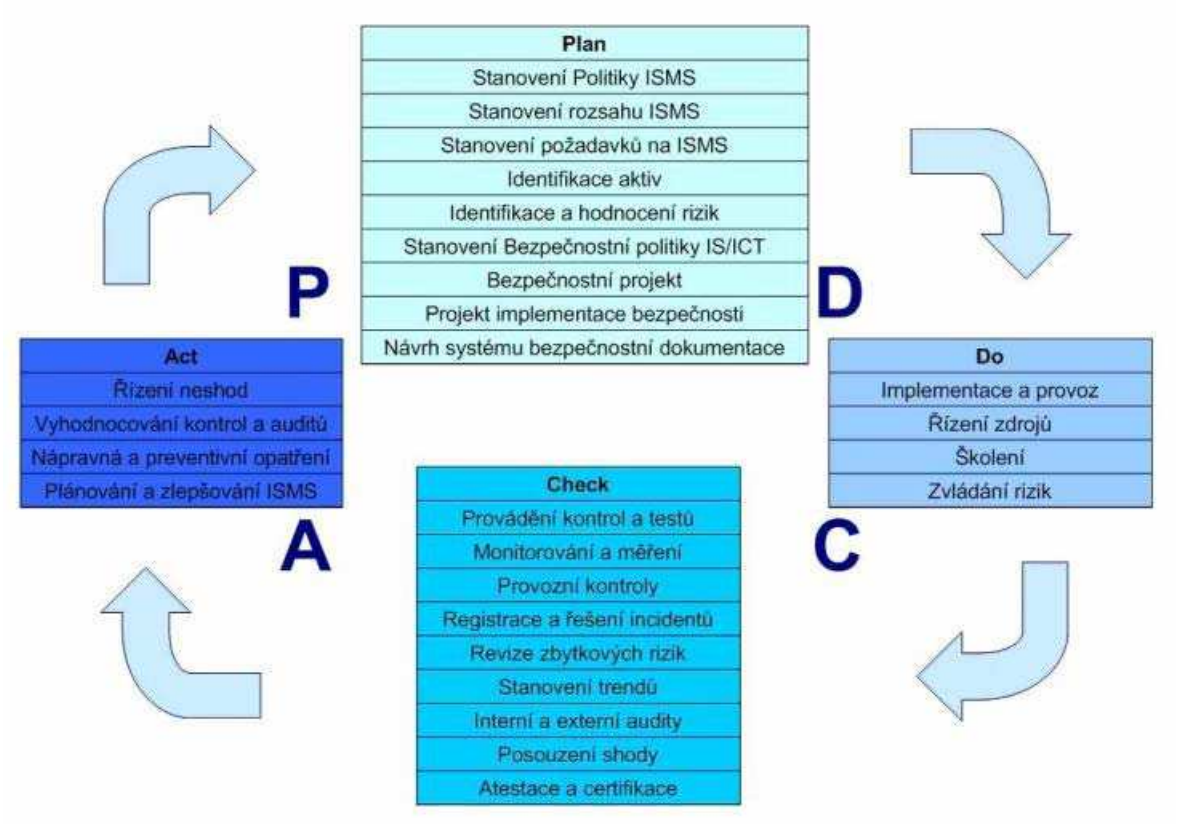
provádění monitoringu a pravidelné revize efektivity ISMS, revize úrovně přijatelných a zbytkových rizik. Provádění interních ISMS auditů a záznamů o dějích a událostech s dopadem na ISMS.

- Jednej

Využití nápravných a preventivních činností, založených na výsledcích analýzy řízení tak, aby bylo dosaženo nepřetržitého zlepšování ISMS. Dosáhnout zlepšení můžeme pomocí implementace identifikovaných vylepšení, prováděním opravných nebo preventivních akcí, využívání zprostředkovaných zkušeností, komunikací se zúčastněnými stranami nad výsledky a zárukou, že implementovanými vylepšeními bylo dosaženo požadovaného cíle.

- **Jednotlivé fáze Demingova cyklu**

Jednotlivé kroky v ISMS, které se musí realizovat v jednotlivých fázích Demingova cyklu – viz. Obr. 5



Obr. 5 Implementace procesů v ISMS [3]

- Plánuj (Plan – P)
- Dělej (Do – D)
- Kontroluj (Check – C)
- Jednej (Act – A)

2.4 Systém managementu bezpečnosti informací

Systém managementu bezpečnosti informací popisují tyto části v normě ČSN ISO/IEC 2700 1/ Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky – část 4 – Systém managementu bezpečnosti informací – část 5 – Odpovědnost vedení – část 6 Interní audity ISMS – část 7 – Přezkoumání ISMS vedením organizace – 8část – Zlepšování ISMS

2.5 Shrnutí managementu bezpečnosti informací

Základem systému managementu bezpečnosti informací je zvýšit bezpečnost vnitřního informačního systému a systematicky řídit bezpečnost firemních informací a to jak vlastních, tak i svěřených zákazníky. Důležitým aspektem v bezpečnosti informačních systémů je, že organizace dosáhne certifikace v oblasti bezpečnosti ICT. Certifikované organizace disponují větší důvěryhodností, jelikož uplatňují postupy v oblasti bezpečnosti ICT.

Cílem zavádění systémů managementu bezpečnosti informací je povýšit tuto oblast mezi jednotně řízené disciplíny v rámci funkčního integrovaného systému managementu.

3 ZPŮSOBY ZABEZPEČENÍ ADMINISTRATIVNÍCH BUDOV

Administrativní budovy, ale i jiné objekty, jako jsou například obytné, obchodní a průmyslové objekty, je zcela nezbytné vhodně zabezpečit proti interním i externím hrozbám. Jejich ochrana musí být stále sledována podle vývoje technologií zabezpečovacích systémů tak, aby bylo možné včas reagovat na případná rizika a popřípadě zamezit trestné činnosti.

3.1 Rozdělení z hlediska ochranných zón

Základní metody ochrany majetku a osob z hlediska ochranných zón lze rozdělit na bariérovou ochranu, perimetrickou ochranu a ochranu budovy.

- Bariérová ochrana

Bariérová ochrana je především tvořena pomocí mechanických zábran, kterými jsou ochranné zdi a ploty. Mechanické zábrany jsou od objektu, administrativní budovy prostorově vzdálené. Cílem bariérové ochrany je zachycení pachatele včas, tj. v okamžiku, kdy ještě nezačal páchat trestnou činnost.

- Perimetrická ochrana

Perimetrická ochrana slouží k zabezpečení volných ploch v hlídaném areálu a k zaznamenávání pohybu neoprávněných osob. Slouží pro střežení rozsáhlých komplexů a budov. Perimetrická ochrana používá nášlapné systémy, sledovací a monitorovací systémy. Nášlapné systémy jsou pod povrchem země a nejsou tedy viditelné. Systém tvoří kabelové nebo hadicové technologie a pracují n principu změny hydraulického tlaku, pasivní kapacity a mikrofonie. Například zemní detekční kabely jsou nejspolehlivějším nášlapným ochranným zařízením. Principem je, že detekční kabel je uložený pod povrchem země, který kolem sebe vytváří až několik metrů široké detekční pole. Narušením pole dojde k vyhlášení poplachu.

Sledovací systémy mají za úkol sledování daného úseku a zaznamenávání pohybu. Systémy jsou tvořeny z mikrovlnných, ultrazvukových a pasivních infračervených detektorů. Pasivní infračervené detektory bývají zabudované do svislých sloupů, které společně vytvářejí perimetrický systém – infračervenou bariéru, infračervené závory, mikrovlnné bariéry.

Monitorovací systémy střeží vymezený prostor pomocí kamer nebo videokamer.

- Plášťová ochrana

Plášťová ochrana spočívá v ochraně pláště budovy a jejích otvorů, jako jsou okna a dveře. K ochraně se používají stejné prostředky ochrany, jako u perimetrické ochrany. Zabezpečují se dveře a skleněné plochy (okna, stěny,…), významnou úlohu mají i a zámkové systémy bezpečnostních dveří.

3.2 Ochrana majetku a osob pomocí integrovaného bezpečnostního systému

Ochrana majetku a osob je zajišťována kombinací fyzické ostrahy, režimových a organizačních opatření a mechanickými a technickými zabezpečovacími prostředky.
Mezi technické prostředky ochrany patří elektrický zabezpečovací systém, elektrická požární signalizace a ústředny, přenosové zařízení (telefonní karty, GSM hlásiče), systém průmyslové ochrany, PCO (dispečink a ústředny).
Mezi mechanické zábranné systémy patří systémy obvodové, plášťové a předmětové ochrany.

3.3 Technické prostředky ochrany

Norma ČSN EN 50131-1 ed.2, s platností od 1. 1. 2009, v českém překladu normy místo dosud používané zkratky EZS je používána zkratka z originálu – I&HAS – poplachové zabezpečovací a tísňové systémy.
V celém rozsahu diplomové práce však uvádím elektrickou zabezpečovací signalizaci pod zkratkou EZS, která je všeobecně známa a doposud používaná. Je i publikovaná v časopisech (např. SECURITY magazín, březen/duben 2010 [20]) a katalozích např. (Elektronické systémy budov, Katalog produktů 2010-2011, Variant plus [23]).

3.3.1 Elektrická zabezpečovací signalizace EZS

Elektrický zabezpečovací systém (dále jen „EZS“) je soubor technických prostředků, ústředna, čidla, signalizační a doplňkové prostředky vytvářející systém, který slouží k včasné signalizaci místa narušení chráněného objektu.
Základem elektronického zabezpečovacího systému je čidlo umístěné v hlídaném prostoru. Čidlem může být magnetický kontakt hlídající otevření dveří nebo oken, prostorové čidlo detekující pohyb v prostoru, otřesové čidlo reagující na náraz, nebo detektor tříštění skla. K většině ústředen EZS lze připojit i detektor kouře, úniku CO nebo jiného unikajícího

plynu. EZS systémy umožňují předání poplachové informace na zvolená místa, čímž usnadní činnost zásahové služby. Navazují na klasickou a režimovou ochranu objektu, doplňují ji a zkvalitňují celkové zabezpečení.

- Drátové systémy EZS

U drátových systémů je náročnější instalace, jelikož je nutné propojení jednotlivých komponentů vodičem. Z tohoto důvodu se doporučuje především do novostaveb. Výhodou je, že není nutné měnit po určité době baterie ve snímačích.

Obr. 6 Drátový systém EZS [25]

- Bezdrátové systémy EZS

Bezdrátové systémy jsou vhodné především do objektů, kde není možná instalace kabeláže. Umožňují snadnou a rychlou montáž a tím zpravidla nedochází k narušení běžného provozu v zabezpečovaných prostorách. U bezdrátových systémů je nutné měnit baterie ve snímačích, na což systém automaticky předem upozorňuje. Výhodou však je snadný způsob instalace a odinstalování systému, například pro případ, kdy je třeba se systémem manipulovat nebo stěhovat. V současné době je již možné kombinovat drátové a bezdrátové prvky zabezpečení.

Obr. 7 Bezdrátový systém EZS [25]

- **Prvky EZS**

Nejčastěji používané prvky EZS jsou prvky obvodové ochrany (infračervené závory, mikrovlnné bariéry, štěrbinové kabely), prvky plášťové ochrany (magnetické kontakty, snímače na ochranu skla, poplachové folie) a prvky prostorové ochrany (pasivní infračervené snímače, ultrazvukové a mikrovlnné snímače, kombinované snímače).

- **Výstupní prvky EZS**

Výstupními prvky EZS jsou vnitřní a venkovní sirény, GSM komunikátory, telefonní hlásiče, grafická nadstavba, tabla, a další.

Obr. 8 Ozvučovací systém [27]

- **Ochranný faktor EZS, vnější i vnitřní ochrana**

Elektronická zabezpečovací signalizace je stavebnicovým systémem, ke kterému je možné přidávat i přídavná zařízení zvyšující nejen komfort ovládání systému, ale i bezpečí osob a majetku. Systémy EZS uživatele chrání před nežádoucími nebo nelegálními vstupy do administrativních budov, kanceláří a dalších objektů i před možnými materiálními škodami. EZS zaznamenávají vstup a pohyb ve střeženém prostoru, objektu a včasnou informací přispívají k minimalizaci případných škod. EZS se dá nastavit na dva druhy signalizace, buď tichá, nebo hlasitá.

- **Opatření, vyhlášení poplachu EZS**

Spustí se vysoký, nepříjemný tón, který má zastrašující nebo šokový efekt na případného pachatele, upozorní okolí, policii a uživatele hlídaného objektu. Okamžitě při poplachu spuštěném EZS systém automaticky zašle poplachovou zprávu o spuštění alarmu bezpečnostní agentuře, v současné době je nezbytnou součástí doplnění systému EZS telefonním hlásičem. Ten dokáže v případě narušení střeženého objektu podat vlastníkovi telefonickou hlasovou nebo SMS zprávu na předvolená telefonní čísla. V případě, že objekt není připojen na pevnou telefonní linku, lze využít pro přenos zprávy o narušení objektu i GSM modul s využitím SIM karty různých operátorů. Spuštěním EZS může případně dojít k vyvolání dalších akcí v návaznosti na jiné systémy, např. zapnutí osvětlení, zablokování elektrických zámků dveří, spuštění okamžitého nahrávání kamerového systému a tak dále. Vyhlášení poplachu vede k zamezení nebo ztížení násilného vniknutí do střeženého objektu.

3.3.2 Elektrická požární signalizace EPS

Systémy elektronické požární signalizace (dále jen „EPS“), tvoří důležitou součást systémů protipožární ochrany objektů a budov. Zajišťují rychlou a včasnou identifikaci a lokalizaci vzniku požáru. Používají se především v místech, kde je třeba místo či objekt zabezpečit proti požáru. Může se jednat a výrobní haly, administrativní budovy, centra a mnoho dalších. Cílem EPS je ochrana lidí a majetku.

Elektrická požární signalizace je plně automatický systém. Jedná se o skupinu technických zařízení, která slouží k tomu, aby detekovala požár již při jeho vzniku a tím rychle přivolala na místo vznikajícího požáru osobu, která je schopna začínající požár zlikvidovat. EPS také umí odemykat a zamykat příslušné vchody a východy, nebo můžou ovlivnit odvětrávání místností, popřípadě systém sám může hasit požár. EPS je již dnes v nových stavbách povinný a u všech ostatních objektů norma stanovuje přímo ty objekty, kde je EPS povinná.

Hlavní části elektrické požární signalizace je tzv. opticko-kouřové čidlo, které detekuje přítomnost kouře. Další součástí systému je siréna. EPS informuje uživatele o vzniku požáru akustickou a optickou signalizací přímo v objektu nebo pomocí zařízení dálkového přenosu. V prašném prostředí se místo opticko-kouřového čidla používají jiné typy, např. ionizační, nebo termodiferenciální, které reagují na prudké zvýšení teploty v hlídaném

prostoru. Nejčastěji používané typy detektorů jsou opticko-kouřový a sledující maximální teplotu + nárůst teploty.

- **Požární hlásiče**

Podle využití a kompatibility s daným systémem, můžeme použít automatické i tlačítkové hlásiče požáru. Dělíme je podle prostředí, pro které jsou určené. Jedná se o hlásiče do normálního i venkovního prostředí a hlásiče s nebezpečím výbuchu.

Výstupní signalizací je siréna. Podle podmínek zabezpečení musíme zvolit i vhodný výstup signalizace. Složitější EPS se dají třeba napojit na pult centralizované ochrany nebo přímo na hasičský záchranný sbor, popřípadě jinou službu.

Obr. 9 Tísňové tlačítko EPS a výstupní signalizace [25]

Autonomní hlásiče požáru jsou varovným prvkem, který je vhodný do pracovních i obytných prostor, jako doplňková výstraha. Využití mají v objektech, kde není možné instalovat vodiče, mají vlastní napájení a interní sirénu.

Obr. 10 Vybrané typy autonomních detektorů [25]

- **Ozvučovací systémy**

Ozvučovací systémy se používají k oslovení co nejširšího okruhu lidí a k ozvučení veřejných prostor. Používání těchto systémů je velmi veliké a to zejména v administrativních budovách, ve výrobních halách, podnicích, letištích, ale i třeba ve školách a úřadech. Jsou určené pro ta místa, kde je třeba informovat, sdělit, upozornit a zejména hlášením pomoci při ochraně osob. Plní také funkci požárního a evakuačního rozhlasu.

Evakuační rozhlas slouží zejména k evakuaci osob při požáru a bezpečnostním ohrožení osob. V případě nebezpečí je automaticky aktivováno evakuační hlášení, které je již dopředu zaznamenané na jednotce digitálního záznamu.

3.3.3 Systém průmyslové ochrany

V dnešní době velmi rychle roste vývoj technologií. Právě v bezpečnostním průmyslu jsou kamerové systémy jedním z nejrychleji se rozvíjejících oborů. Tyto systémy se dnes používají při zabezpečení vnitřních i vnějších prostor. Kamerové systémy se stávají stále vyhledávanějším prvkem bezpečnostních systémů. Nejčastěji jsou právě kamerové a záznamové zařízení využívána v kombinaci s přístupovým systémem a elektrickým zabezpečovacím systémem což zaručuje efektivnost a větší bezpečnost daného objektu.

Kamerový systém je významným prostředkem pro monitorování a to nejen pro bezpečnostní účely. Slouží i pro ověření poplachového stavu nebo pro sledování různých výrobních procesů. Uzavřený televizní okruh umožňuje sledovat střežené prostory a přenášet obraz z více míst do jednoho dohledového centra.

Kamerový systém tvoří různé typy kamer, zobrazovací zařízení, zařízení na zpracování, záznam obrazu popřípadě zvuku, přenosové cesty, příslušenství a doplňky.

Kamerové systémy pro vnitřní prostory se používají zejména v obchodních, nákupních, zábavních a sportovních centrech, ve výrobních halách a průmyslových podnicích, v administrativních budovách, hotelích, garážích a na letištích.

Použití kamerového systému vnějších prostor se používá zejména k monitorování armádních objektů, pro sledování parkovišť, benzínových pump, letišť dále i k sledování objektů a pozemků, využití je i u státních budov, muzeí a dalších objektů.

Obr. 11 Kamerový systém [25]

Obr. 12 Jednotlivé části CCTV systému [25]

- **CCTV kamerové systémy**

CCTV kamerové systémy používají speciální videorekordéry, které umožňují dlouhodobý bezobslužný záznam obrazu z bezpečnostní kamery.

Dříve se používaly analogové videorekordéry, ty jsou nyní postupně vytlačovány digitálními videorekordéry, které ukládají obrazová data na pevný disk. Digitální videorekordéry jsou vybaveny videoserverem, který umožňuje vzdálený přístup k rekordéru přes LAN / Internet.

- **IP Kamery**

IP kamery se v současné době stále více s rozvojem digitalizace signálu a zvyšování přenosové kapacity IP sítí prosazují na našem trhu. Můžou nabídnout vyšší rozlišení (megapixelové kamery, v současnosti max. 8MPix) a tím zajistí výrazně větší množství detailů v zaznamenaném obraze pro pozdější vyhodnocení. IP kamera obsahuje kromě standardní analogové videokamery také integrovaný videoserver, který zajišťuje digitalizaci a komprimaci videosignálu pro připojení kamery k počítačové síti.

Aplikace IP kamer bývá výhodná zvláště u velkých systémů a to především z pohledu ceny, jelikož jejich nevýhodou je celkově vyšší cena. Naopak výhodou je větší variabilita v souvislosti s rozšiřováním systému.

IP kamery nám umožňují generovat videostream, který je možné přenášet po IP síti a zálohovat v podstatě kdekoli například v centralizovaném datovém centru. Pomocí implementovaného webserveru sledování živého obrazu pomocí standardních webovských prohlížečů v zásadě z kteréhokoliv místa v síti (LAN / Internet). Lze využít i pro videomonitoring a zabezpečení vzdálených objektů.

3.4 Mechanické zábranné systémy MZS

Mechanické zábranné systémy (dále jen „MZS“), tvoří základní část bezpečnostního systému. Účelem MZS systémů je zabránění popřípadě ztížení vniknutí do chráněného prostoru a ochrany majetku před poškozením, krádeži či odcizením, pomocí překážek a bariér.

Podle druhu ochrany můžeme hovořit o těchto systémech MZS

- Obvodová ochrana slouží pro ohraničení hlídaných prostor, patří sem zejména zdi a ploty, brány, vrata a bezpečnostní dveře, závory a další.
- Plášťová ochrana zahrnuje bezpečnostní mříže a skla, dále bezpečnostní folie na skla a další.
- Předmětové ochrana, hovoříme o prostředcích, které mohou sloužit k individuální ochraně nebo, jako samostatné úschovné objekty. Jedná se o bezpečnostní trezory a skříně, pokladny, kontejnery, kufry a další.
- Sabotážní ochrana zabezpečuje jednotlivé komponenty zabezpečovacího zařízení proti úmyslnému či neúmyslnému poškození.

V současné době je třeba využívat k zabezpečení objektů i mechanické zábranné systémy, které vedou ke zvýšení celkové bezpečnosti firem, úřadů, administrativních budov a jiných objektů. Je však třeba si uvědomit i s ohledem na rostoucí kriminalitu, že tyto systémy je nezbytné kombinovat i s dalšími bezpečnostními systémy tak, aby byla zaručena bezpečnost budov, jako celku.

3.5 Organizační a režimová opatření

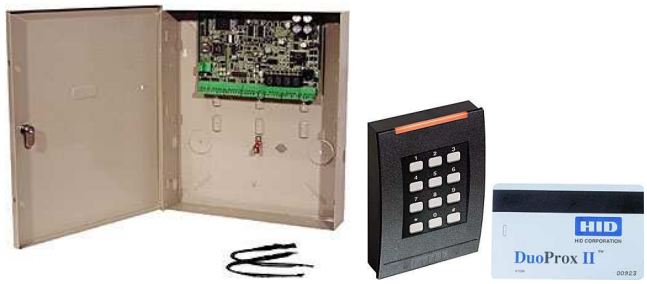
Organizační opatření jsou uplatňována pomocí norem, směrnic, interních směrnic a řádů společnosti. Režimová organizační opatření mohou být vnější a vnitřní. Mezi vnitřní opatření můžeme například zařadit kontrolovaný pohyb osob ve střeženém objektu a kontrolovaný pohyb osob na parkovišti. Vnější režimová opatření zahrnují kontrolu vstupu a výstupu u zabezpečovaných objektů a to jak osob, tak i vozidel.

3.5.1 Elektronická kontrola vstupu EKV (ACS)

Systém kontroly vstupu (dále jen „EKV“) slouží k zabezpečení vstupů a zajištění vstupního režimu do daného prostoru. Je určený k elektronickému prokazování oprávněnosti vstupu a totožnosti osob. V současné době se využívá především bezkontaktních karet či čipů nebo biometrických snímačů často v kombinaci s PIN kódem.

Podstatou EKV je zabránění přístupu neoprávněných osob do vyhrazených prostor a zabránění přístupu k důležitým či utajovaným informacím. Kontrola vstupu nám dále umožní sledování pohybu osob v definovaných zónách, vyhledávání a kontrolu osob v jednotlivých průchodech v objektu.

Začíná být zcela běžné, že zákazník vyžaduje pro zabezpečení svého objektu, možnost ovládání systému EZS systémem kontroly vstupu. Systém kontroly vstupu bývá často vázán na EPS. Prvky kontroly vstupu se převážně integrují do systémů domácích telefonů a videotelefonů. Systém kontroly spolu s použitím mechanických zábranných prostředků zlepšuje podmínky k zajištění režimu vstupu a zefektivnění výkonu ostrahy. Jeho použití výrazně snižuje ztráty na pracovišti a značně zvyšuje produktivitu práce.



Obr. 13 Komponenty přístupového systému [25]

- **Kontrola docházky**

Vedle funkcí kontroly vstupu se ve společnostech evidují i důvody odchodu ze zaměstnání, tedy docházky. Docházka zároveň umožňuje lepší kontrolu a přehled nad příchody, odchody a celkovou odpracovanou dobou zaměstnanců. Nejdůležitější je úroveň software, který umožňuje předzpracování zaznamenaných dat. Tyto docházkové systémy se navrhují individuálně dle potřeb společnosti. Pro kontrolu docházky se nejčastěji používají karty, bezkontaktní čipy a čím dál častěji se setkáváme s biometrickými snímači.

Důležitou součást kontroly vstupu a docházky tvoří i zámkové systémy. Elektromechanické zámky jsou určené pro různé typy dveří a pro velkou škálu použití. Motorické zámky a elektromagnetické zámky, slouží ke správné funkci zámků. V kombinaci s bezpečnostním kováním tvoří samozamykací zámky důležitý bezpečnostní prvek a zároveň nekomplikují přístup do objektu. Nezbytné jsou z hlediska ochrany majetku, ale i z hlediska bezpečnosti.

- **Kontrola obchůzky**

Systém kontroly obchůzky je zařízení, které se využívá ke kontrole činnosti strážní služby. Základem jsou čipy, které jsou upevněné ve speciálních držácích na trase obchůzky.
Ostraha musí přiložit při každé obchůzce snímač ke každému čipu na trase a snímač zaznamená místo a čas jeho pohybu.
Jsou dvě možnosti řešení a to, že údaje o pohybu ostrahy se uloží do snímače a později se přenesou ke zpracování do PC nebo přenos dat probíhá on-line přímo do PC, tím řešením se snižuje riziko ztráty dat.

- **Biometrické systémy**

Biometrické systémy pracují na základě automatické autentizace. Systém je založený na jedinečnosti osobnosti člověka, kde výhodou jsou neměnitelné biologické charakteristiky, tím je také zaručená velká bezpečnost. Zařízení nemá žádné ovládací prvky, k identifikaci slouží snímač. Tato metoda je vysoce spolehlivá a ekonomicky nenákladná.
Využívá se zejména metod otisku prstů nebo scanu duhovky oka.

- Metoda otisku prstů

Metoda otisku prstů je dnes považována za jednu z nejspolehlivějších identifikačních metod. Používají se rozlišovací metody detekce teplotních rozdílů, případně přímého optického snímku nebo metody měření nepatrných změn. Snímače otisků prstů, pracují na principu otisku prstu, jsou to snímače optoelektronické, kapacitní a termodynamické.

- Scan duhovky oka

Scan duhovky oka je založený na jedinečnosti člověka, který je schopen zajistit vysokou bezpečnost střeženého objektu. Princip je založený na uložení jedinečné charakteristiky duhovky uživatele do databáze oprávněných osob, kterým je umožněný vstup do zabezpečeného prostoru. Snímky oka vytvoří zařízení podobné digitální kameře a pak je zpracuje speciální software. Výhodou je téměř nulová pravděpodobnost chyby a jednoduchost v používání tohoto systému.

- Další způsoby identifikace

Další způsoby identifikace můžou být pomocí geometrie ruky nebo obličeje, ušního boltce, dynamiky podpisu, podle hlasu a další.

Obr. 14 Čtečka biometrická, otisk prstu [27]

Obr. 15 Čtečka duhovky oka [27]

3.5.2 Domovní dorozumívací systémy DDS

Domovní dorozumívací systémy (dále jen „DDS“) jsou zařízení, která pomáhají k zabezpečení objektu. Může se jednat, jak o komerční budovy, kanceláře, tak i o byt nebo dům.

Kamerová jednotka videotelefonu je instalována buď u vchodových dveří do objektu nebo na oplocení či bráně. Videotelefon je uvnitř objektu a to na libovolném místě, podle potřeby a využití systému. Kamerová jednotka videotelefonu a videotelefon jsou vzájemně propojeny kabelem. Displej videotelefonu zobrazuje osobu, která se snaží do objektu dostat. Komunikace je zajištěna pomocí mikrofonu a reproduktoru, výhodou je, že lze

s osobou komunikovat, aniž bychom otevřeli dveře. Z pohledu bezpečnosti se jedná o výhodu především z pohledu zabránění nechtěného vniknutí do objektu.

Mezi DDS systémy zahrnujeme komunikační systémy, domácí audio a videotelefony, interkomy.

Obr. 16 Domácí telefony a videotelefony [25]

3.6 Fyzická ochrana

- Ostraha

Ostraha kontroluje a provádí dozor a dohled nad dodržováním veřejného pořádku a norem občanského soužití, slušného chování a dobrých mravů v areálu klienta a provádí opatření k zabránění jejich narušování. Vykonává kontrolní činnost v dohodnutých místech budovy. V případě přijetí poplachové informace je povinna zjistit příčinu poplachu a provést základní kroky vedoucí k eliminaci poplachu. V případě přijetí jakékoliv informace o mimořádné události, jako je požár, porucha elektrického zařízení, fyzický konflikt, je povinna učinit kroky k minimalizaci škod na majetku klienta. Ostraha vede protokol o průběhu služby, kam zaznamenává všechny důležité údaje.

- Bezpečnostní služba

Bezpečnostní pracovníci jsou povinni, zejména informovat svého nadřízeného, při mimořádné situaci a chránit majetek a zdraví osob v areálu. Řešit každý bezpečnostní incident či mimořádnou událost, tj. provést prvotní opatření k zabránění vzniku škody či jiné újmy, následně událost objasnit, vyšetřit a přijmout adekvátní opatření zabraňující jejímu opětovnému výskytu. Řádně provádět bezpečnostní procedury na jednotlivých stanovištích a aplikovat nastavená bezpečnostní logistická opatření a dohlížet na jejich dodržování. Také znát, uplatňovat a dodržovat interní normy areálu, požární směrnice objektu, hygienické zásady.

3.7 Příklady z praxe

Praktické příklady zabezpečení administrativní budovy a zabezpečení pomocí kamerového systému je uvedeno v příloze diplomové práce (PI, PII a PIII). Obrázky (Obr 17, Obr 18 a Obr 19) jsou v příloze diplomové práce PI, PII a PIII.

- PI.: Obr. 17 Příklad zabezpečení budovy, perimetrická ochrana

Obrázek zobrazuje prostorové uspořádání perimetrického systému.

- PII.: Obr. 18 Příklad zabezpečení inteligentní budovy

Obrázek zobrazuje příklad malé administrativní budovy a možnosti využití jednotlivých prvků zabezpečení, jejich možnou pozici a variabilitu. Ukazuje na jednoduchém příkladu jednotlivé prvky EZS, EPS, přístupového systému a vnějšího obvodového zabezpečení.

- PIII.: Obr. 19 Příklad zabezpečení objektu pomocí kamerového systému

Obrázek zobrazuje schéma kabelového propojení jednotlivých prvků CCTV systému s vazbou na „lokální“ počítačovou síť a jednotlivé dohledové PC.

3.8 Shrnutí zabezpečení administrativních budov

Administrativní budova, která má sloužit pro společnosti, které disponují velkými objemy dat a informací z jakékoliv oblasti podnikání, musí v dnešní době splňovat základní bezpečnostní kritéria. Majitel budovy musí zajistit vnitřní i vnější ochranu, pomocí dostupných zabezpečovacích mechanismů a to do takové míry, aby byla schopna zaručit bezpečnost společnosti a zajistila si tak důvěru potencionálních pronajímatelů nemovitosti.
Současným trendem se stávají dobře zabezpečené tak zvané inteligentní budovy. Na našem trhu stále více stoupají do popředí, kde klíčovou vlastností je právě kompatibilita řídicích systémů.
Cílem realizace inteligentní budovy je integrace čtyř základních oblastí provozu do jednoho funkčního systému. Jedná se o oblasti, efektivního využívání energie, zabezpečovacích systémů, telekomunikačních systémů a automatizace pracovišť. Nedílnou součástí je i inteligentní elektroinstalace.
Jednou z výhod inteligentních budov je jejich kvalita, která zajisté přispívá ke zvýšení efektivnosti a produktivity práce ve společnosti. Výhody inteligentních budov jsou i ekonomické, jelikož se minimalizují provozní náklady a náklady na energii.

II. PRAKTICKÁ ČÁST

4 NÁVRH BEZPEČNOSTI INFORMAČNÍCH A KOMUNIKAČNÍCH TECHNOLOGIÍ PRO V SW SPOLEČNOSTI

Praktická část diplomové práce je koncipovaná, jako realizační projekt pro zabezpečení „virtuální“ SW Společnosti, za smyšlených podmínek a stavů. Práce je zaměřená na návrh zabezpečení informačních a komunikačních systémů, ostatní aspekty, jako ekonomické, finanční, zde nejsou zohledněny.

V současné době není možné použít materiály konkrétní společnosti, jako podklad pro diplomové práce, protože v oblasti bezpečnosti se jedná o citlivá, velmi citlivá, důvěrná, tajná a neveřejná data (viz. Zákon 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti). Z tohoto důvodu jsem k práci přistoupila, jako k návrhu možného realizačního projektu, pro menší nebo středně velkou IT společnost. Práce je logicky rozdělena na tři části vzhledem k nárokům na zabezpečení softwarové společnosti, jako celku (viz. Kapitola 4.2. Návrh realizace zajištění pro SW Společnost).

Celý projekt vychází ze skutečnosti, že SW Společnost i administrativní budova jsou tzv. imaginární.

4.1 Definice společnosti

Název společnosti: SW Společnost, s.r.o.

Sídlo společnosti: Ulice 123, Brno 602 00

SW Společnost, s.r.o. se zabývá dodávkou a implementací informačních technologií, systémů a služeb. V současné době má 50 zaměstnanců a sídlí ve starší administrativní budově bez možnosti rozšíření pracovních míst. Jsou zde zavedeny pouze základní bezpečnostní technologie, jako jsou EZS, trezor a klíčový systém.

SW Společnost, s.r.o. získala významnou zakázku pro státní správu a tím i zahraničního investora, se kterým plánuje v nejbližší době stěhování do nových prostor v nové čtyřpatrové administrativní budově v centru Brna. Počítá se s tím, že SW Společnost, s.r.o. obsadí celé jedno patro budovy a přijme nové zaměstnance do celkového počtu 150 zaměstnanců. Vzhledem, k tak vysokému počtu zaměstnanců, stěhování do nových prostor a práce na zakázce pro státní správu je SW Společnost, s.r.o. nucena po dohodě s investorem investovat do vlastního zabezpečení.

Vzhledem k těmto okolnostem výše popsaných, bude vypracovaný projekt vnitřní a vnější bezpečnosti, která popisuje a navrhuje vhodná řešení zabezpečení pro SW Společnost, s.r.o. v nové administrativní budově.

4.2 Návrh realizace zajištění bezpečnosti pro SW Společnost

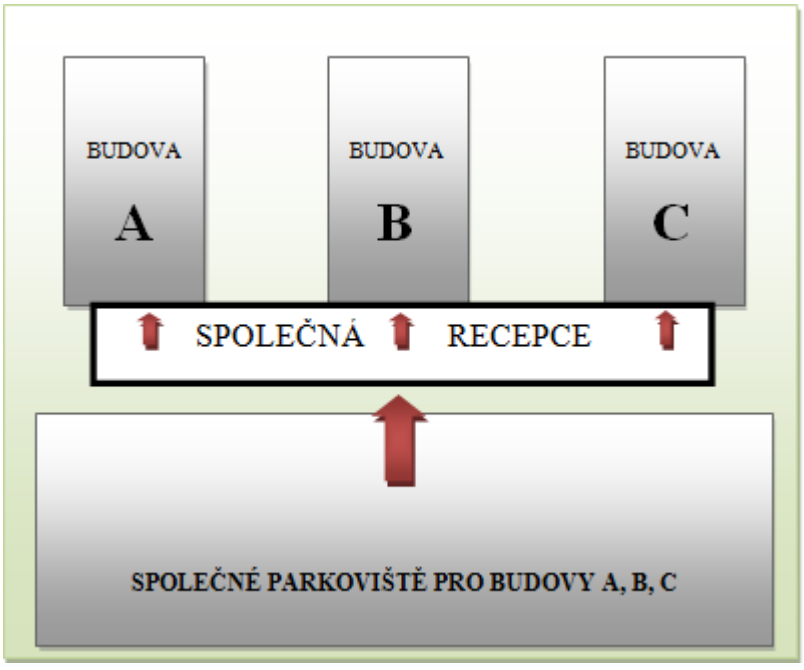
1. **Zajištění vnější bezpečnosti na úrovni budovy**
   a. Definice administrativního komplexu
   b. Provozní řád
   c. Legislativa
   d. Systémy zabezpečení budovy
      - Telefonní a datové rozvody
      - Systém průmyslové ochrany
      - Elektronická kontrola vstupu
      - Elektronický požární systém
      - Elektronický zabezpečovací systém
      - Ozvučení veřejných prostor, požární rozhlas
      - Parkovací systém
      - Obchůzkový systém
      - Fyzické zabezpečení, ostraha objektu
2. **Zajištění vnitřní bezpečnosti na úrovni prvního patra administrativní budovy**
   a. Popis a plánek patra
   b. Definice klíčových míst zabezpečení
   c. Návrh technologií pro klíčové oblasti
      - Telefonní a datové rozvody, strukturovaná kabeláž
      - Elektronický zabezpečovací systém
      - Systém průmyslové ochrany
      - Elektronický požární systém
      - Elektronická kontrola vstupu
3. **Zajištění vnitřní bezpečnosti na úrovni systémů a práce SW Společnosti**
   a. Popis současného stavu ICT systémů
   b. Návrh změny uspořádání a propojení ICT systémů
   c. Definice umístnění klíčových technologií
   d. Návrh řešení zabezpečení oblastí
      - Datová a hlasová komunikace
      - Internet, vzdálený přístup
      - Hardware
      - Software
      - Administrativa bezpečnosti

4.3 Zajištění vnější bezpečnosti na úrovni administrativní budovy

4.3.1 Definice administrativního komplexu budov

Administrativní budova je navržena tak, aby splňovala podmínky a požadavky nadefinované SW Společností, s.r.o. Předpokládáme tedy, že administrativní budova je součástí nového komplexu budov. Celý komplex se skládá ze tří sektorů budov A, B a C, které jsou navzájem propojené. K celému komplexu budov patří i společné parkoviště. Ve společném vestibulu budov je umístěna jedna centrální recepce pro všechny budovy, více viz. Obr. 20 Schéma administrativní budovy s parkovištěm. Jednotlivé budovy A, B a C mají čtyři nadzemní podlaží. Převážná část objektu slouží, jako kancelářské prostory. Ostatní prostory jsou využívány jako sklady a malé obchody.

Uvažuji tak, že nově postavený komplex budov má jediného vlastníka, kterým je společnost SB, s.r.o., která je i zároveň správcem budov. Tyto budovy byly postaveny jako tak zvané „inteligentní budovy“. Pojmem inteligentní budovy rozumíme takové budovy, které mají jednotlivé systémy navzájem propojeny do jednoho komplexního celku tak, aby došlo jak k úsporám nákladů investičních, tak i provozních.



Obr. 20 Schéma administrativní budovy s parkovištěm

4.3.2 Provozní řád administrativní budovy

- Provoz budovy

Komplex budov bude otevřený 24 hodin denně se zvláštním režimem. V pracovních dnech od 6.00 hodin do 20.00 hodin - budova plně přístupná. Mimo tuto denní dobu, budou některé systémy zablokovány a v případě potřeby se bude muset kontaktovat ostraha objektu. O víkendu a o svátcích bude mít nastavený stejný režim, tedy jako mimo pracovní dobu.

Parkoviště u budovy bude přístupné přes jeden závorou chráněný vstup i výstup, který bude elektronicky připojen do systému EKV budovy. Platit zde bude stejný řád, jako u provozu budovy, tak je popsáno výše.

Vstup do budovy v době jejího uzamčení bude možné pouze za předem definovaných podmínek. Do budovy bude mít povolený vstup pouze ten člověk, který je zaměstnancem některé z firem v daném objektu. Takový člověk bude vybavený vstupní kartou pro vstup do objektu a pin kódem. Člověk, který není zaměstnancem některé z firem v této administrativní budově a chce za nějakým účelem vstoupit do budovy mimo dobu jejího otevření, tak bude povinen pomocí zvonku přivolat ostrahu, zvonek bude umístěn před vchodem do budovy s řádným označením strážní služba. Ostrahu bude také možné zavolat pomocí telefonního čísla uvedeného na vstupu do budovy. Strážní služba ověří danou osobu podle daných pokynů a eviduje vstup do budovy do knihy návštěv.

Odchod z budovy v době jejího uzamčení bude možné podle předem nadefinovaných podmínek. Při ochodu z budovy zaměstnanci použijí kartu a pin kód. Při odchodu jiné osoby z budovy bude nutné přivolat ostrahu, která zajistí odemknutí dveří, po té strážní služba eviduje odchod z budovy do knihy návštěv.

- Ostraha objektu

Ostraha objektu strážní službou bude zajištěna 24.00 hodin denně se smluvně zajištěnou specializovanou společností. V nočních hodinách v pracovních dnech od 20.00 hodin do 6.00 hodin a o víkendech a svátcích 24 hodin denně strážní služba bude vykonávat pravidelné obchůzky a to minimálně 1x za tři hodiny a v případě nutnosti i častěji. Ostraha sleduje prostřednictvím kamerového systému stav objektu. V případě zjištění nedostatků či závad, sepíše záznam, který dá k dispozici majiteli objektu. Kontakt na strážní službu bude vyvěšený u vstupních dveří do budovy.

- Recepce ve vstupní hale administrativní budovy

Ve vstupní hale do administrativní budovy se předpokládá recepce. V prostoru recepce bude umístěna informační tabule, která poskytuje informace o rozmístění firem v objektu. Budou zde umístěné také poštovní schránky a trezor. Dále se počítá s nápojovým automatem a klidovou zónou, kde budou umístěné stoly a křesla pro návštěvy.

V pracovní dny od 6.00 hodin do 20 hodin bude na recepci k dispozici recepční. Jejím úkolem bude podávat základní informace o firmách, které jsou v daném komplexu, zejména v jakém patře či budově se firma nachází. Návštěvě, která půjde za nějakým účelem do některé z firem, poskytne návštěvnickou cedulku s řádným označením, například „NÁVŠTĚVA“. Návštěvu zapíše do určené knihy i s údaji z občanského průkazu. Zapůjčí ji vstupní kartu do budovy a telefonicky bude kontaktovat zástupce společnosti. Provoz recepce o víkendu, svátcích a mimo pracovní dobu v pracovních dnech, službu bude nepřetržitě zajišťovat ostraha 24 hodin denně, v rámci daných služeb.

- Bezpečnostní opatření vstupů do kanceláří

Nájemci budou předány majitelem budovy klíče od kanceláří po uzavření nájemní smlouvy, nájemce si pak musí zajistit vstup do kanceláří tím, že si zajistí nové klíče od kanceláří výměnou zámků a zajistí bezpečný vstup do objektu kanceláří, například vstupním docházkovým systémem. Pro případ mimořádné události, jako například vzniku výbuchu nebo požáru, úniku vody nebo plynu, bude muset nájemce předat majiteli budovy náhradní klíče a vstupní kódy ke všem dveřím. Všechny klíče a údaje ke vstupům do kanceláří budou uložené v zapečetěné obálce v trezoru. Obálka bude řádně označená jménem firmy. Trezor bude umístěný v recepci budovy.

V případě mimořádné události, bude moci obálku porušit majitel nebo strážní služba. O této mimořádné události bude muset strážný provést záznam s důvodem zásahu. V případě, že nájemce v průběhu svého nájmu vymění klíče či jiné vstupní zabezpečení, bude jeho povinností dát klíče k dispozici opět v zapečetěné obálce, která bude řádně označena jménem firmy a po tom uložena zpět do trezoru. Nebude-li v případě mimořádné události umožněný vstup do objektu kanceláří, tak nájemce ponese odpovědnost za vzniklou škodu a to v plném rozsahu.

- Poštovní služby

Nájemci budovy budou při podpisu nájemní smlouvy předány klíče od schránky. Schránka bude řádně označena obchodním jménem firmy a to do doby trvání nájemní smlouvy.

Poštovní schránky budou umístěné ve vstupní hale administrativní budovy hned vedle recepce. Obyčejnou poštu bude mít na starosti recepční, která bude třídit poštu podle jednotlivých firem a bude ji třídit do poštovních schránek dané firmy. V případě doporučené pošty, pošty do vlastních rukou nebo balíků roznášet bude zaměstnanec České pošty přímo na recepci firmy, pro kterou je zásilka určená.

- Údržba a opravy pronajatých prostor v administrativní budově

Pronajímatel bude moci provádět veškeré opravy a údržbu, které budou nadefinované v nájemní smlouvě. Jednalo by se především o opravy elektrické instalace, osvětlení, včetně výměny žárovek, opravy topného systému a oken a dveří a prací s tím souvisejících. Údržby toalet.

Nájemce bude moci ve svých pronajatých prostorách provádět činnosti, jako je malování pronajatých prostor, rozvod sítí LAN, pokládka koberců, nebo jiných podlahových krytin, zabezpečení vstupu, dveří, pověšení předmětu na stěny, jako jsou obrazy, nástěnky. Po ukončení nájemní smlouvy bude muset nájemce uvést všechno do původního stavu.

- Kouření v objektu

V celé administrativní budově bude platit zákaz kouření.

- Parkování

Pronajímateli budou přidělena podle nájemní smlouvy parkovací místa.

Parkoviště se předpokládá hlídat 24 hodin denně a to ostrahou a monitorovacím zařízením. Parkoviště bude i vybaveno elektrickou závorou.

Vstup na parkoviště bude nadefinovaný podle platných pravidel pronajímatele. Na parkoviště budou mít povolený vjezd, jen ty vozidla, která se prokážou, že mají vymezené parkovací stání. Majitel takového místa bude vybavený elektronickou kartou, kterou si otevře závoru ke vstupu na parkoviště. Předpokládám, že na parkovišti bude vymezeno i několik míst pro návštěvy. V případě, že bude chtít na parkoviště vjet návštěva, tak její vjezd bude muset povolit ostraha, která zároveň tuto návštěvu zaeviduje. U závory bude také nainstalovaný zvonek, na který návštěva zazvoní a do hlásiče nahlásí patřičné údaje.

Odjezd z parkoviště bude nadefinovaný podle platných pravidel pronajímatele a budou platit stejná pravidla, jako při vjezdu na parkoviště.

Nájemce bude povinen udržovat parkovací místo v čistotě. Dodržovat bezpečnost parkovaní a veškeré předpisy vztahující se k bezpečnosti a ochraně zdraví, protipožární a hygienické a další předpisy. Dále zabezpečit vlastní majetek proti odcizení, neponechávat předměty v autě, které by mohly zapříčinit možné vloupání či odcizení.

- Úklidová služba

Úklid bude zajišťovat úklidová služba a to v celé budově ve všech kancelářích. Režim úklidu bude ve všední dny denně a to od 16 hodin. Úklidová služba bude mít stanovená pravidla, jakým způsobem úklid provádět. Především se bude jednat o vyprazdňování odpadkových košů a vysávání koberců, mytí podlah v prostorách toalet, úklid a doplnění potřebného materiálu, otření prachu z pracovních stolů zaměstnanců.

Z bezpečnostního hlediska se nedoporučuje uklízet PC a jeho příslušenství a další možné elektrické zařízení. Úklid pracovních stolů se nebude provádět v případě, že se na stolech budou vyskytovat osobní věci nebo pracovní prostředky zaměstnance. Dále z bezpečnostního hlediska úklidová služba nebude zalévat květiny v kancelářích a vstupovat do uzamčených prostor.

- Stěhování

Pro stěhování nábytku či jiného kancelářského vybavení, bude moci nájemce použít pouze vchod do budovy, který bude ze zadní strany budovy, přístupný pouze z parkoviště. Z bezpečnostních důvodů bude zakázané stěhování hlavním vchodem budovy a parkováním před tímto vchodem.

- Legislativa

Veškeré systémy vnitřního a vnějšího zabezpečení budovy proti externím a interním hrozbám se budou muset podřídit normám a platným předpisům v době realizace prací a zejména normám a požadavkům platných při odběru elektrické energie a vydaných rozvodným závodem a dále požadavkům telekomunikačního úřadu a hasičského záchranného sboru, jakož i jejich požadavkům.

4.3.3 Návrh norem pro použití při zabezpečování budov

ČSN 34 2300	Předpisy pro vnitřní rozvody sdělovacích vedení
ČSN 34 3100	Bezpečnostní předpisy pro obsluhu a práci na el. zařízeních
ČSN 33 1500	Elektrotechnické předpisy. Revize el. zařízení
ČSN 33 1600	Elektrotechnické předpisy. Revize a kontroly el. ručního nářadí během používání
ČSN 33 2000-1	El. Zařízení - Základní ustanovení
ČSN 33 2000-4-41	El. Zařízení - Ochrana před úrazem el. proudem
ČSN 33 2000-4-481	El. Zařízení - Ochrana před úrazem el. proudem podle vnějších vlivů
ČSN 33 2000-4-482	El. Zařízení - Ochrana proti požáru

ČSN 33 2000-5-51	El. Zařízení - Výběr a stavba el. zařízení, všeobecné předpisy
ČSN 33 2000-5-52	El. Zařízení - Výběr soustav a stavba vedení
ČSN 33 2000-5-54	El. Zařízení - Uzemnění a ochranné vodiče
ČSN 33 2000-5-56	El. Zařízení - Napájení zařízení sloužících v případě nouze
ČSN 33 2000-7-707	El. Zařízení - Požadavky na uzemnění v instalacích zařízení pro zpracování dat
ČSN 73 0802	požární bezpečnost staveb – nevýrobní objekty
ČSN 33 2030	Ochrana před nebezpečnými účinky statické elektřiny
ČSN 33 2130	Elektrotechnické předpisy – Vnitřní elektrické rozvody
ČSN 33 2180	Připojování el. přístrojů a spotřebičů
ČSN 34 0350	Pohyblivé přívody a šňůrová vedení
ČSN 34 1090	Prozatímní el. zařízení
ČSN 34 1390	Předpisy pro ochranu před bleskem
ČSN 34 3108	Bezp. předpisy o zacházení s el. zařízením pracovníky seznámenými
ČSN 36 0020-1	Sdružené osvětlení
ČSN 36 11-3	Měření umělého osvětlení
ČSN 36 0450	Umělé osvětlení vnitřních prostorů
ČSN 36 15..	Bezpečnost el. ručního nářadí (řada norem)
ČSN ISO 38640	(ČSN 01 8010) Bezpečnostní barvy a bezpečnostní značky
ČSN EN 60073	Elektrotechnické předpisy. Kódování sdělovačů a ovládačů pomocí barev a doplňkových prostředků
ČSN IEC 446	Elektrotechnické předpisy. Značení vodičů barvami, nebo číslicemi

4.3.4 Přehled předpisů BOZP, které musí být při návrhu, provádění a užívání dodrženy a splněny

Zákon č. 1/1993 Sb. Ústava ČR

Zákon č. 1/1991 Sb. O zaměstnanosti ve znění pozdějších předpisů

Zákon č. 277/2003 Sb. O technických požadavcích na výrobky a o změně a doplnění některých zákonů

Zákon č. 455/1991 Sb. O živnostenském podnikání ve znění pozdějších předpisů

Zákon č. 513/1991 Sb. Obchodní zákoník ve znění pozdějších předpisů

Zákon č. 550/1991 Sb. O všeobecném zdravotním pojištění ve znění pozdějších předpisů

Zákon č. 174/1968 Sb. O státním odborném dozoru ve znění pozdějších předpisů

Zákon č. 71/1967 Sb. O správním řízení ve znění pozdějších předpisů

Zákon č. 65/1965 Sb. Zákoník práce ve znění pozdějších předpisů

Zákon č. 40/1994 Sb. Občanský zákoník ve znění pozdějších předpisů

Zákon č. 20/1966 Sb. O péči a zdraví lidu v úplném znění vyhlášeném v č. 86/1992 Sb.

Zákon č. 109/2001 Sb. O územním plánování a stavebním řádu (stavební zákon)

Zákon č. 238/1991 Sb. O odpadech ve znění zákona č. 300/1995 Sb.

Vyhláška MZd č. 48/1982 Sb., kterou se stanoví základní požadavky k zajištění bezpečnosti práce a technických zařízení, ve znění pozdějších předpisů

Vyhláška MZd č. 20/2001 Sb. O vytváření a ochraně zdravých životních podmínek ve znění pozdějších předpisů

Vyhláška č. 20/1979 Sb., kterou se určují vyhrazená elektrická zařízení a stanoví některé podmínky k zajištění jejich bezpečnosti, ve znění vyhlášky č. 553/1990 Sb.

Vyhláška č. 83/1976 Sb. O obecných technických požadavcích na výstavbu, ve znění pozdějších předpisů

Vyhláška č. 85/1976 Sb., o podrobnější úpravě územního řízení a stavebním řádu, ve znění vyhl. 155/1980 a 378/1991 Sb.

Vyhláška č. 369/2001 Sb., kterou se stanoví obecné technické požadavky zabezpečující užívání staveb osobami s omezenou schopností pohybu a orientace

Vyhláška č. 64/1984 Sb. O hygienických zásadách pro práci s chemickými karcinogeny, doplněné výnosem MZSV č. 76/1990

Vyhláška č. 13/1977 Sb. O ochraně zdraví před nepříznivými účinky hluku a vibrací

Nařízení vlády ČR č. 192/1988 Sb. O jedech a jiných látkách škodlivých zdraví (vč. žíravin)

Hygienický předpis MZd sv. 39/1978 – směrnice č. 46 O hygienických požadavcích na pracovní prostředí

Hygienický předpis MZd sv. 58/85 – směrnice č. 66, kterou se mění sm. č.46/78 v části týkající se nejvyšších přípustných koncentrací v prac. ovzduší

Hygienický předpis MZd sv. 51/81 – směrnice č. 58 O základních hygienických požadavcích, o nejvyšších přípustných koncentracích nejzávažnějších škodlivin v ovzduší a ohodnocení stupně jeho znečištění

Hygienický předpis MZd sv. 66/89, výnos č. 74 MZD, kterým se mění směrnice č. 46/78, týkající se nejvyšších přípustných koncentrací aerosolů, prachů s různými účinky

Hygienický předpis MZd sv. 37/77, směrnice č.41-43, týkající se hluku a vibrací

Nařízení vlády č. 495/2001 Sb., kterým se stanoví rozsah a bližší podmínky poskytování osobních ochranných pracovních prostředků, mycích, čisticích a dezinfekčních prostředků.

4.3.5 Systémy zabezpečení budovy

V této části realizačního projektu popisuji zajištění vnější bezpečnosti na úrovni budovy pomocí základních bezpečnostních systémů.

V nově vybudované „smyšlené“ administrativní budově najdeme již moderní systémy bezpečnosti, které jsou již zavedené před nastěhováním společnosti a tím tedy splňují zásadní podmínky pro nastěhování SW Společnosti, s.r.o. Systémy budou využity a popřípadě propojeny s navrhovaným řešením zabezpečení samotných prostor SW Společnosti, s.r.o.

- **Centrální místo dohledu, recepce**

Popis napojení systémů na recepci areálu a hlavní serverovnu je popsáno u jednotlivých systémů zabezpečení.

- **Spolupráce slaboproudých zařízení s nadřazeným řídicím systémem inteligentní budovy**

Jednotlivé slaboproudé ústředny a zařízení budou pracovat autonomně a přes svá síťová rozhraní a budou umožňovat přenos dat na řídicí systém inteligentní budovy, který umožní vzájemné sdílení dat jednotlivých zařízení a systémů a současně provede jejich vizualizaci. Centrální dohledová PC stanice s vizualizačním programem bude umístěna v centrální recepci a prostorech správy budovy. Přenos dat řídicího systému bude probíhat po technologické strukturované kabeláži, které povede napříč objektem a bude fyzicky oddělena od počítačových sítí jednotlivých nájemců. Jednotlivá pracoviště budou mít diferencovaný přístup k datům podle předem stanoveného oprávnění.

- **Telefonní a datové rozvody**

Předpokládám, že všechny budovy administrativního komplexu budou vybaveny jednotným telekomunikačním systémem, jehož cílem bude zajistit dostupnost, jak hlasových, tak i datových služeb v jednotlivých částech budovy.

Pro interní komunikaci se plánuje vybudování strukturované sítě, která bude sloužit pro rozvod telefonu a počítačové sítě. Jedná se o univerzální rozvodný systém hvězdicového typu, který se používá pro přenos dat, hlasu a videa. Centrální datový rozvaděč včetně aktivních prvků bude umístěn v hlavní rozvodné místnosti serverovně, která bude hned

vedle recepce. Rozvod se plánuje zrealizovat v kategorii odpovídající potřebné a predikované rychlosti přenosu různých výrobců CAT6.

Pro minimalizování rušivých impulsů nebo možnosti zničení systému z důvodu přepětí, které může být způsobeno bleskem, nebo jinou formou statické elektřiny nebo i nepřímým účinkem těchto vlivů bude, jako ochrana proti přepětí realizováno použití přepěťových ochran a vodičů přepětí. Přepěťové ochrany musí být instalovány podle předpisů a doporučení výrobce.

Přívod státních linek bude proveden do telefonního rozvaděče, který je součástí hlavní serverovny objektu, tedy do jednoho centrálního místa s distribucí do podružných míst a center.

Pro provoz administrativní části se nainstaluje moderní robustní telefonní ústředna. Tato ústředna bude vybavena analogovými a digitálními pobočkami. Tyto pobočky se využijí pro provoz budov. Na základě požadavků nájemců jednotlivých nájemních úseků bude možné ústřednu doplnit až na 5000 pobočkových linek. V provozním zázemí administrativní části budovy se plánují rozvody dat a telefonů provést ve strukturované kabeláži kategorie 6. Strojovny a místnosti technologií v suterénu budou mít telefonní zásuvky RJ12. V každé strojovně výtahu také bude telefonní zásuvka pro připojení telefonu ve výtahu. Systém musí splňovat národní komunikační předpisy pro provoz telekomunikačních zařízení, tak jak jsou předepsány Českým telekomunikačním úřadem, jakož i mezinárodní doporučení organizací ITU či CCITT.

- **Nouzové telefonní spojení z výtahových kabin**

Zajištění nouzového volání z kabin výtahů bude zajištěno po telefonních linkách centrální ústředny. Ve výtahových kabinách se nainstalují univerzální dveřní telefony. V případě poruchy výtahu bude umožněno přímé volání do místnosti bezpečnostní služby, tedy na recepci budovy, kde bude obsluha přítomna po celých 24 hodin. Rozvod k rozvaděčům výtahů se provede samostatným telefonním rozvodem. Univerzální dveřní telefony budou připojeny z elektrických rozvaděčů výtahů, po vedení které, je součástí výtahů.

- **Telefonní a datová rozhranní jednotlivých pater a součástí budovy**

Cílem je, aby se mohli všichni nájemci napojit na telefonní rozvaděč popřípadě pobočkovou ústřednu, na základě dohody se správou budovy. Rozvody telefonů a strukturované kabeláže i s úložnými systémy v nájemních úsecích budou prováděny na základě uživatelských změn na náklady nájemce.

U vstupů do budovy, u vjezdové brány a u závor pro vjezd a výjezd na parkoviště budou nainstalována tabla domácích telefonů pro dálkové uvolňování těchto vstupů. Tabla domácích telefonů sloužících pro provoz budovy, se napojí na pobočkovou telefonní ústřednu budovy. Ze vstupů se uživatel dovolá do centrální recepce. Od závor se účastník v případě potřeby taktéž dovolá do centrální recepce. Pro možnost otvírání dveří do nájemních částí administrativní budovy budou na dveřích ve výtahových lobby nainstalována tabla domácích telefonů a napojí se na telefonní rozvaděče v místnostech stoupaček. Podle požadavku nájemce je možné tabla napojit na pobočkovou ústřednu nájemce, nebo na pobočkovou ústřednu budovy a propojit je na požadované linky.

- **Domácí telefon**

Pro hlasovou a obrazovou komunikaci s návštěvníky bude vybudován moderní domovní telefonní systém. Systém zabezpečí komunikaci s návštěvníky od vstupu nebo vjezdu do objektu. Použijí se tabla s hovorovým modulem, se dvěma tlačítky, povětrnostním krytem a nosnou krabicí. Z tabla centrální recepce bude možné se dovolat na všechny místa. Obsluha podle provozního režimu budovy manuálně vpustí návštěvu do budovy. Hlavní vstup bude vybaven el. posuvnými dveřmi. Tablo u hlavního vstupu do budovy bude umístěno na plášti budovy a tabla u vjezdů a výjezdů na parkoviště se umístí na sloupcích spolu se čtečkami přístupového systému.

- **Systém průmyslové ochrany**

Předpokládám, že objekt je vybaven kamerovým systémem. CCTV, systém se skládá ze systému bezpečnostního, který doplňuje EZS a EKV, a ze systému provozního, zajišťujícího kontrolu, zejména opatření k zamezení krádežím. Oba systémy však bude možné vzájemně kombinovat a využívat společně. Celý komplex kamer pak může sloužit pro obě aplikace. Pro CCTV systém bude použitý maticový přepínač a digitální záznamové zařízení se záznamem na pevný disk, který obsahuje detektor pohybu a výstup, jak pro monitor, tak pro PC.

CCTV systém lze doplněním příslušných vstupních nebo výstupních karet rozšířit až na 64 kamer a 8 monitorů. Ve standardním provedení lze připojit až 8 ovládacích klávesnic, 32 alarmových vstupů a 6 výstupů. Záznamové zařízení lze také rozšířit doplněním dalšího zařízení, které se síťově připojí na stávající systém. Kapacita systému lze rozšířit doplněním vícekapacitního disku.

Pro sledování vnějších prostorů okolo objektu a na střeše předpokládáme, že budou použity kamery pro venkovní prostředí.

Venkovní kamery budou vybaveny objektivy s automatickou clonou s ohledem na proměnlivé světelné podmínky. Vnější kamery se umístí do povětrnostního krytu s vytápěním. Kamery budou umístěny převážně v prostorech určených pro veřejnost a kontrolu pojízdných ploch v objektu parkoviště, kde se umístí i kamery s ANTIVANDAL krytem pro zamezení případného napadení a poškození kamery.

V centrální recepci budou nainstalované 2x 2 monitory 19“ s plochou obrazovkou LCD, na nichž se plánuje sledování jednotlivých kamer. Další dva monitory LCD 19“ budou umístěny v místnosti správy budovy.

Pro přepínání kamer slouží přepínací jednotky, vybavené záznamovým zařízením pro evidenci událostí. Celý systém spolupracuje s EZS a v případě narušení objektu, v době mimo provoz se provede automaticky záznam z příslušné kamery. Systém spolupracuje taktéž s EPS. Dohledový systém bude modulární s možností případného rozšíření.

Ústředna CCTV systému resp. záznamové zařízení, je základním článkem celého systému. Plní funkci centrálního prvku, umožňuje sloučení všech kamer z objektu do jednoho celku. Umožňuje tzv. triplexní záznam, kdy v jednom okamžiku je možné prohlížet, sledovat a editovat záznam. Při jeho návrhu bude nutné počítat s možným dalším rozšířením.

- **Záznamové zařízení**

Doba záznamu záznamového zařízení bude minimálně sedm pracovních dnů. Umožní nám tak okamžitý přístup k záznamu, spouštění záznamu přes zabudovaný detektor pohybu umístěný v kameře, zabudovaný časový rozvrh, triplexní provoz s možností přehrávání, nahrávání i živý obraz v jednom přístroji, s možností propojení s EZS, externí výstupy pro poplachové stavy, záznam na harddisk, 3 úrovně hesel, možnost přenosu signálu po různých sítích a na různá záznamová média, možnost ovládání přes PC.

- **Vnitřní kamera pevná**

Při návrhu zabezpečení klíčových míst vstupu a výstupu do administrativní budovy a vstupech do dílčích částí budov a jednotlivých pater se celkem plánuje využití 47 vnitřních kamer.

Bude zde použitá vnitřní kamera v provedení černobílá pevná digitální, rozlišení 480 řádek, citlivost 1 lux, 1/2" CCD, optika vari-focus, napájení 230V AC a signál po koaxiálním vedení, aktivace kamery na základě vlastní detekce aktivity, detekce ztráty videosignálu se signalizací u hlavní ostrahy, včetně standardního krytu s kamerovým nástěnným držákem.

- **Venkovní kamera pevná**

Při návrhu pro zajištění plášťové ochrany budovy, hlídání parkoviště a monitoringu důležitých míst okolo objektu bude použito celkem 18 venkovních kamer.

Konkrétní technické řešení zajistí venkovní kamera černobílá pevná digitální, rozlišení 480 řádek, citlivost 1lux, 1/2" CCD, optika vari-focus, napájení kamery a kamerového krytu 230V AC + signál po koaxiálním vedení, aktivace kamery na základě vlastní detekce aktivity, detekce ztráty videosignálu se signalizací u hlavní ostrahy, s polokulovým krytem a kamerovým nástěnným držákem.

4.3.6 Elektronická kontrola vstupu EKV (ACS)

Systém kontroly vstupu v administrativní části budovy se sestává z použitých bezkontaktních čteček na vybraných vstupech a východech. Jejich funkcí je zamezení přístupu nepovolaných osob do uzavřených částí budovy a dále stanovení různých druhů oprávnění vstupu mezi jednotlivými pracovníky.

Instalovány budou v důležitých technických prostorech, jako jsou vstupy do administrativních podlaží a dalších.

Použijí se jednostranné i oboustranné prostupy. Oboustranný prostup definuje přesně čas příchodu a odchodu v těchto vybraných prostorách a je trvale zaznamenán v paměti událostí, V některých místech bude pouze jednostranný vstup, odchod se realizuje odchodovým tlačítkem nebo klikou.

Pro identifikaci se použijí magnetické karty, čtečky a budou osazeny v montážních boxech ve zdech, na dveřních rámech, anebo na sloupcích poblíž vchodu do budovy. Ve dveřích s EKV se nainstalují elektrické zámky a magnetické kontakty. Magnetické kontakty se napojí do systému EZS. Pro ovládání vjezdových a výjezdových zařízení (vjezdová a výjezdová závora, brána na vjezdu do objektu) budou nainstalovány čtečky karet a tabla intercomu na sloupcích závor a na vstupu vedle vjezdové brány.

Ústředna systému bude počítačový server se softwarem umístěný v centrální serverovně. Pro zprávu systému a výdej karet se plánují v budově ještě dvě pracovní stanice. Jedna v prostorech správy budovy a druhá pro výdej karet v centrální recepci. Pro ovládání systému bude k dispozici řídící a grafický software. Ovládací jednotky EKV se umístí podle potřeb u kabelových stoupaček v návaznosti na kapacitu zařízení. Napájení bude zálohované místně pomocí záložního zdroje s akumulátorem.

Kabelové rozvody EKV se provedou vodiči FTP CAT5E. Elektrické zámky dveří budou napojeny reverzně tak, aby pod proudem byly zamčeny, napájeny budou ze zdrojů 24V s akumulátorovou zálohou. V prostorech budou dveřní čtečky napájeny z baterií a čtečky ve zdi z traf 24V zálohovaných z diesel generátoru.

Zařízení EKV bude systémově propojené s EPS, v případě požáru odblokování elektrických zámků, elektrických závor a podobně.

Přístupový systém musí obsahovat všechny funkce požadované u blokování vstupů - kategorizace přístupových práv, časová omezení, monitorování stavů vstupů v reálném čase.

Systém EKV bude vytvořen především pro integraci do firemních podnikových sítí a následně informačních systémů. Data systému pak mohou být sdíleny v reálném čase kterýmkoli oprávněným uživatelem. Výkonná, flexibilní a modulární architektura systému umožní jeho snadné rozšiřování a přizpůsobování představám a požadavkům uživatele. Kapacita systému po přidání řídících jednotek na sběrnici bude až 256 čteček, 30 000 držitelů karet a možnost připojení až na 1000 vzdálených míst. Takový systém umožní připojit až 4 pracovní stanice v síti LAN. Sběr dat a poplachů v reálném čase může probíhat přes server systému. Modulárnost systému umožní sestavit celé řešení pouze z řídících jednotek, které budou vybaveny přídavnými moduly podle přesných požadavků systému. K dispozici bude kompletní řada přídavných modulů s poplachovými vstupy/výstupy, komunikační, pro připojení čteček a klávesnic.

Součástí celé instalace budou tři kusy závor, včetně jejich řídících jednotek, vybavených vstupem pro požární otevření systémem EPS. Signál EPS bude předán ve formě beznapěťového kontaktu. Závory budou dále vybaveny indukční smyčkou v podlaze, která zabrání uzavření vozidla těmito závorami a zkontroluje správný průjezd.

4.3.7 Elektronický požární systém EPS

Elektrická požární signalizace v objektu bude navržena na základě požadavku požárního specialisty, jako součást vybavení objektu, sloužící ke včasnému zjištění možného vzniku požáru, včasného varování osob a minimalizace škod.

Při realizaci EPS bude vhodné použití následujících typů zařízení:

- Opticko-kouřové hlásiče, které slouží k detekci viditelných kouřových aerosolů vznikajících pyrolytickým hořením zejména plastických hmot a materiálů na bázi PVC. Vykazují lepší citlivost na detekci bílých kouřů než ionizační.

- Tepelné hlásiče, které slouží, jako klasický hlásič požáru a reaguje na překročení maximální teploty nebo rychlosti zvyšování teploty okolí nebo diference teploty. Vzhledem k nižší citlivosti a pomalé indikaci požáru je vhodný tam, kde nelze instalovat jiné typy hlásičů.
- Tlačítkové hlásiče, jsou určeny k manuálnímu ohlášení požáru osobou. Umisťují se v únikových cestách ve výšce 1050 - 1500mm od podlahy na přístupném a viditelném místě. Tlačítkové hlásiče s možností individuální adresace bývají zapojeny na poplachovou linku společně s hlásiči automatickými.
- Lineární teplotní diferenciálně-maximální hlásič je systém, pracující na principu vyhodnocování změny tlaku plynu v uzavřeném systému, způsobeném rozpínáním plynu při ohřívání měděné snímací trubice.
- Lineární tepelný hlásič, kabelážní systém EPS, pracující na základě změny elektrického odporu v důsledku změny teploty okolí senzorového kabelu. Používá se na sledování stavu v prostoru zdvojených podlah a v prostorech před patrovými elektro místnostmi.
- Adresné moduly, slouží pro načítání dat do systému EPS z kontrolovaných systémů (SHZ) a dále se používají pro ovládání prvků přes reléové přepínací výstupy (požární klapky, dveře, rozvaděč silnoproudu), resetování hlásičů v podzemních podlažích.

- **Provedení EPS v administrativní budově**

Pro použití v objektu bude nainstalován analogový redundantní adresovatelný systém EPS, který bude řádně homologován pro použití v ČR a splňující požadavky podle platných norem. Ve vytypovaných prostorách podle požadavků požárního specialisty a návrhu projektanta budou umístěny hlásiče požáru opticko-kouřové, v kuchyňkách a prostorách s možností zakouření hlásiče tepelné.

Automatické opticko-kouřové hlásiče budou kromě stropů umístěny také v prostorech nad podhledy a také tam, kde je vyšší požární riziko vzniklé větší integrací kabelových rozvodů. Čidla budou zapojena do kruhových oboustranně napájených požárních linek. Hlásiče se upevní na podhledy, na stropy v podhledech, v suterénech a prostorách bez podhledů na stropech. Montáž bude provedena tak, aby bylo zajištěno jejich snadné zkoušení, čištění a byla možná výměna montážní tyčí.

Na únikových cestách ve všech podlaží se umístí tlačítkové hlásiče pro manuální vyhlášení poplachu. Adresné moduly s reléovými přepínacími kontakty pro ovládání požárních klapek v nadzemních podlažích a pro ovládání dveří se připevnění na zdi v místnostech

elektro stoupaček. V těchto místnostech v nadzemních podlažích bude na zdi připraven vstupně/výstupní adresný modul pro připojení tepelného lineárního systému pro kontrolu zdvojených podlah v chodbách před stoupačkami. Teplotní lineární systém bude nainstalován v případě, že budou nájemci ve zdvojených podlahách, nainstalovány rozvody strukturované kabeláže.

V nájemních prostorech budou na stropě nainstalovány opticko-kouřové hlásiče EPS se sirénou v patici hlásiče. V případě detekce kouře se siréna aktivuje a hlásič předá informaci ústředně EPS. Ve společných chodbách budou na zdi pod stropem nainstalovány světelné majáky, které budou v případě požáru blikat.

Adresné moduly pro načítání dat ze SHZ budou umístěné ve strojovnách SHZ.

Napájecí zdroje EPS budou v administrativní části centrální recepce a ve stoupačkách.

- **Ústředna EPS**

Ústředna EPS bude umístěna v hlavní serverovně budovy, kde se zajistí stálá obsluha 24 hodin a současně bude sloužit, jako ohlašovna požáru v objektu. Ústředna se také propojí se systémem správy budovy.

Hlásičům budou přiřazeny software a hardware adresy podle pořadí na lince a podle sestavení skupin v návaznosti na požární úseky a střežené prostory.

- **Vyhlášení evakuace**

Vyhlášení evakuace se předpokládá automatické, pomocí nahraných zpráv v systému požárního rozhlasu. Obsluhou pomocí požárního a evakuačního rozhlasu, evakuace proběhne podle místa požáru a podle požární zprávy. Dále odblokováním únikových východů jištěných systémy EZS a EKV.

4.3.8 Elektronický zabezpečovací systém EZS

Pro zabezpečení objektu proti vloupání bude použito robustního a dostatečně dimenzovaného systému, s plášťovou ochranou v 1.NP a vstupů do nadzemních podlaží. Střeženy budou vstupní prostory do nájemních jednotek, a to provizorně do doby pronajmutí. Poté může nájemce svůj lokální systém napojit na domovní systém pomocí instalovaných koncentrátorů.

Napojení kancelářských prostor v nadzemních podlažích na systém EZS bude umožněno v patrových slaboproudých rozvaděčích, kde bude ponechána délková rezerva kabelu sběrnice systému. Systém se bude dát rozšířit přidáním koncentrátorů (až 64) až na 512 zón, 32 klávesnic.

V navrženém systému EZS bude realizováno 5 stupňů ochrany. Tomu odpovídá členění detektorů do jednotlivých zón:

- Zóny tvořící plášťovou ochranu obvodu objektu
- Zóny tvořící prostorovou ochranu uvnitř objektu
- Zóny tísňové ochrany osob
- Zóny předmětové ochrany
- Zóny autoochrany proti sabotáži

Pro administrativní část objektu bude počítáno s využitím všech pěti stupňů ochrany.
Objekt bude vybaven:

- Vstupní dveře budou opatřeny magnetickými kontakty, prosklené dveře budou chráněny detektory tříštění skla.
- Vstupní prostory budou chráněny infrapasivními detektory.
- Okna budou chráněna detektory tříštění skla a otevíratelná okna magnetickými kontakty

Nainstalována bude i plně adresovatelná ústředna, která komunikuje s jednotlivými čidly pomocí vzdálených modulů (koncentrátory) a bude ovládána jednak z panelu ústředny, tak i z pomocných klávesnic s prosvětlenými displeji, rozmístěnými po budově.
Ústředna bude vybavena náhradním zdrojem a rozhraním pro sériovou tiskárnu. Použijí se všechny čtyři linky, kterými systém disponuje. Tyto linky budou nataženy ve čtyřech stoupačkách a zakončeny zakončovacími rezistory. Na linkách budou napojeny přímo koncentrátory a klávesnice, které jsou adresovatelné do systému.
Tří vstupy koncentrátorů se využije pro hlášení poruch v systému MaR. Prostřednictvím EZS bude stálá služba informována o potížích v MaR i v mimopracovní době.
Klávesnice budou instalovány v hlavní recepci, u vstupu do prostor správy budovy a v každé již pronajímané jednotce. Koncentrátory budou umístěny poblíž připojovaných detektorů v podhledech. Ústředna se připojí na náhradní zdroj budovy. Všechny kabeláže budou provedeny s dostatečnou délkovou rezervou, aby umožňovali lokální přemístění. Detektory se napojí do domovní centrály EZS přes koncentrátory nad podhledem, které mohou být podle přání nájemníka zaměněny za jeho nezávislou ústřednu. Ta může zůstat napojena na PCO objektu.
V objektu bude nepřetržitá 24 hodinová služba (recepce), proto není uvažováno s propojením na hlídací bezpečnostní službu.

4.3.9 Ozvučení veřejných prostor

Ozvučení veřejných prostor umožňuje přehrávání hudby na pozadí, reklam, osobních vzkazů ve veřejných prostorách a koridorech. Plní také funkci požárního a evakuačního rozhlasu v souladu s platnou normou.

S ohledem na požární zprávu bude zajištěno, aby výstražná signalizace byla dostatečně srozumitelná při vzniku kritické události.

Celková koncepce ozvučení vychází z rozvodů požárního rozhlasu, který bude instalován, jak ve veřejných prostorech, tak i v pronajatých kancelářských jednotkách. Požární rozhlas bude rozdělen do oblastí tak, aby umožňoval provést evakuaci.

V případě vzniku požární situace bude požární zvuková signalizace nadřazena ostatní zvukové produkci.

- **Ústředna ozvučení**

Digitální mikroprocesorová ústředna bude instalovaná pro administrativní část v hlavní serverovně. Ústředna umožní směrování hlášení do samostatných reprodukčních zón, odpovídajících požárním úsekům, přepínání zdrojů a mluveného slova z ovládacích pultů, telefonní ústředny či modulů předehraných zpráv. Spínáním výstupů z ústředny EPS budou do vybraných prostorů předávány požární a evakuační instrukce.

Výkonová část ústředny bude osazena zesilovači s nominálním výkonem 100-200-400W.

Všechny tyto komponenty se umístí v rozvaděči hlavní serverovny spolu s ústřednou, řídicím systémem a výkonovým zesilovačem. Přepážkový mikrofon bude umístěn v hlavní recepci. Systém požárního rozhlasu má svůj záložní zdroj a bude napájený ze sítě 230V z rozvodů zálohovaných diesel generátorem.

- **Provedení ozvučení**

Pro funkci požárního hlášení budou umístěny reproduktory na společném prostranství, jako v kancelářích, prodejních jednotkách, technických místnostech a všech prostorách s trvalým pobytem osob.

Reproduktory se použijí stropní, do podhledu 2,5 – 5 - 10W , eventuelně skříňkové nástěnné 10 W. Kabelové rozvody budou provedeny bezhalogenovými kabely pro hlášení požáru, nepodporujícími hoření. Kabely nebudou uloženy ve společných trubkách nebo žlabech s ostatními slaboproudými rozvody.

4.3.10 Parkovací systém

Na vjezdu na parkoviště se instalují závory pro vjezd a výjezd z parkoviště. Závory budou ovládány čtečkou zapojenou do přístupového systému EKV budovy. V případě problému se uživatel může přes domácí telefon, zabudovaný na sloupku u vchodu do budovy vedle vrat, napojený v rámci telefonních rozvodů dovolat do místnosti ostrahy, případně do centrální recepce administrativní budovy.

Parkovací systém bude nadefinovaný z těchto částí:

- Vjezdový terminál se závorou na vjezdu
- Výjezdový - čtecí terminál se závorou na odjezdu
- Detektory vozidel – indukční smyčky
- Směrová fotozávora na vjezdu a výjezdu pod závorou
- Řídící jednotka se software

Na sloupcích čtecího zařízení vjezdu a výjezdu budou nainstalovány čtečky karet a tablo domácího telefonu (intercom). Uživatel parkoviště přes čtečku karet autorizovanou kartou zvedne závoru a je mu umožněn vjezd, případně výjezd.

V centrální recepci bude ovládací panel závor. Tímto panelem bude možné na dálku otevřít bránu a zvednout závory.

Parkovací systém bude propojen s ústřednou EPS a při výskytu požáru dojde k otevření odjezdových závor. Kabelové rozvody budou provedeny ohniodolnými kabely pro hlášení požáru, nepodporujícími hoření.

4.3.11 Obchůzkový systém

V prostorách budovy bude nainstalován obchůzkový systém. Tento systém slouží k přesné kontrole obchůzky strážných a k časové evidenci všech vykonaných obchůzek. Systém se skládá z kontrolních bodů, osobních čipů, snímače, rozhraní pro ukládání informací z osobních čipů do počítače a z programového vybavení nainstalovaného na počítači.

Počítač s programovým vybavením bude umístěn v místnosti ostrahy. Kontrolní body se rozmístí na základě požadavků správy budovy.

4.3.12 Recepce budovy

V centrální serverovně budou umístěny všechny ústředny pro provoz administrativní části budovy. V recepci bude zajištěná 24 hodinová obsluha. Z recepce také bude možné ovládat a kontrolovat všechny slaboproudé systémy.

Veškeré elektrické napájecí rozvody 230V 50Hz budou zálohované z diesel generátoru. Každý počítač a ústředna bude mít svůj náhradní zdroj (UPS) minimálně na dobu 10 minut než naběhne diesel generátor.

V recepci bude umístěna podlahová krabice. Do krabice se přivedou přímo z operačního centra kabely pro napojení požárního rozhlasu a také kabely strukturované kabeláže a EZS. V recepci bude umístěn externí ovládací panel, klávesnice a tísňové tlačítka EZS a pracoviště EKV pro výdej karet a mikrofonní pultík pro požární rozhlas.

4.3.13 Fyzické zabezpečení, ostraha objektu

- **Obecné zásady výkonu služby ostrahy**

Obecnou povinností bezpečnostní služby bude udržování provozního pořádku, zajištění bezprostřední ochrany osob a majetku budovy. Bezpečnostní služba zajišťuje ochranu majetku a osob v souladu se zákonnými pravomocemi.

Bezpečnostní pracovníci jsou povinni, zejména:

- Informovat svého nadřízeného, při mimořádné situaci a chránit majetek a zdraví osob v areálu.
- Aplikovat nastavená bezpečnostní logistická opatření a dohlížet na jejich dodržování
- Řádně provádět bezpečnostní procedury na jednotlivých stanovištích.
- Řešit každý bezpečnostní incident či mimořádnou událost, tj. provést prvotní opatření k zabránění vzniku škody či jiné újmy, následně událost objasnit, vyšetřit a přijmout adekvátní opatření zabraňující jejímu opětovnému výskytu.
- Nastupovat do služby ve stavu umožňujícímu řádný výkon služby.
- Vystupovat během služby vnímavě a ohleduplně.
- Znát, uplatňovat a dodržovat interní normy areálu, požární směrnice objektu, hygienické zásady.
- Zásady bezpečnosti a ochrany zdraví při práci.
- Řádně provádět osobní kontroly osob opouštějící objekt.

Bezpečnostním pracovníkům je zakázáno, zejména:

- Vzdalovat se ze stanoviště bez svolení nadřízených osob nebo jinak rozptylovat svou pozornost, vykonávat činnost nesouvisející s výkonem služby, jako například přijímat soukromé návštěvy, vést soukromé telefonické hovory.
- Požívat alkoholické nápoje, omamné, toxické a halucinogenní látky před a během služby.

- Přebírat jakýkoliv materiál určený správci budovy a jeho nájemcům, přebírat do úschovy jakékoli předměty, zvířata a písemnosti. Uvedené se nevztahuje na nálezy zaměstnanců a ostatních osob, taktéž se nevztahuje na doručenou poštu, tyto předměty včetně pošty převezme strážce, který zajistí předání majiteli, pokud to není možné, odevzdá nález oprávněné osobě, která zastupuje zájmy klienta.
- Konzultovat s novináři situace nebo problémy související s činností správy budovy a jejich nájemci.
- Používat služební komunikační prostředky k soukromým účelům. Tento zákaz se týká nejen neoprávněného používání telefonů, mobilních telefonů, domovních, respektive dalších telefonů k vedení soukromých hovorů, či odesílání nebo přijímání soukromých SMS. Vztahuje se i k neoprávněnému využití služebního připojení do sítě Internetu. Podobně se zakazuje k soukromým účelům využívat služební prostředky výpočetní techniky.
- Přijímat jakékoliv „věcné či peněžité“ dary od zaměstnanců správy budovy.
- Zaměstnancům bezpečnostní služby je zakázáno uschovávat na vrátnici jakékoliv věci zaměstnanců správy budovy, mimo věcí, které spadají pod majetek budovy.

- **Funkce ostrahy**

Ostraha vede protokol o průběhu služby, kam zaznamenává všechny důležité údaje. Týká se to také jednotlivých důležitých hlášení strážců, všech bezpečnostních incidentů, změn ve složení ostrahy. Tento dokument bude sloužit, jako interní spis bezpečnostní služby.

Ostraha bude vykonávat kontrolní činnost v dohodnutých místech budovy.

V případě přijetí poplachové informace bude povinna zjistit příčinu poplachu a provést základní kroky vedoucí k eliminaci poplachu.

V případě přijetí jakékoliv informace o mimořádné události (požár, porucha el. zařízení, fyzický konflikt) bude povinna učinit kroky k minimalizaci škod na majetku klienta.

Ostraha zavede tzv. knihu vzkazů, která se uloží v místnosti recepce. Do této knihy se zapíšou veškeré připomínky ze strany správy budovy k ostraze objektu, provozní změny a jiné aktuality, bezodkladně po zjištění události.

V případě vzniku aktuálních situací bude odpovídat ostraha za navázání komunikační součinnosti mezi správou budovy, vedením bezpečnostní služby a dalšími zainteresovanými stranami, či osobami.

Úkolem ostrahy je zejména:

- Ostraha kontroluje a provádí dozor a dohled nad dodržováním veřejného pořádku a norem občanského soužití, slušného chování a dobrých mravů v areálu klienta a provádí opatření k zabránění jejich narušování.
- Ostraha kontroluje a provádí dohled, aby nedocházelo k rozkrádání a poškozování zboží a jiného majetku klienta, v takové činnosti pachatelům zabraňuje.
- Podle pokynů oprávněných zástupců správy budovy provádí ostraha kontrolu dodržování pracovní kázně, kontrolu opatření, aby ze strany zaměstnanců nedocházelo k rozkrádání zboží a majetku.
- Ostraha kontroluje to, aby do skladových a administrativních prostor budovy nevstupovaly nepovolané osoby a zabraňuje jejich neoprávněnému vstupu.
- Ostraha kontroluje, aby do objektu nevstupovaly osoby s pojízdnými prostředky (kola, koloběžky, brusle,…).
- Při provedení jakéhokoli zákroku, (použití obraných opatření apod.) je ostraha povinna zajistit a zjistit totožnost případných svědků zákroku, zpracovat záznam o důvodech a průběhu zákroku a předat odpovědnému zástupci správy budovy a vedení bezpečnostní služby, došlo-li při zákroku ke zranění osoby, poskytnout první pomoc a následně lékařskou pomoc.
- Vyžadují-li to okolnosti případu, je ostraha povinna zajistit místo činu, proti znehodnocení kriminalistických stop pro jsoucí šetření orgánu Policie České republiky.
- Při své činnosti je každý strážce povinen zachovávat diskrétnost a mlčenlivost před nepovolanými osobami o skutečnostech, o nichž se dozví a o informacích získaných v souvislosti s výkonem služby. Informace mohou být poskytnuty jen vedení společnosti.

4.4 Zajištění vnitřní bezpečnosti na úrovni patra

4.4.1 Popis prvního patra administrativní budovy

Podle návrhu řešení vnějšího zabezpečení administrativní budovy, již nyní vím, jakými ochrannými prostředky a systémy bezpečnosti bude budova disponovat. Z těchto informací musím vycházet při návrhu řešení vnitřního zabezpečení prvního patra administrativní budovy, do které se bude stěhovat SW Společnost, s.r.o.

Níže popíši návrh konkrétního řešení zabezpečení celého 1. patra v sektoru A komplexu administrativních budov.

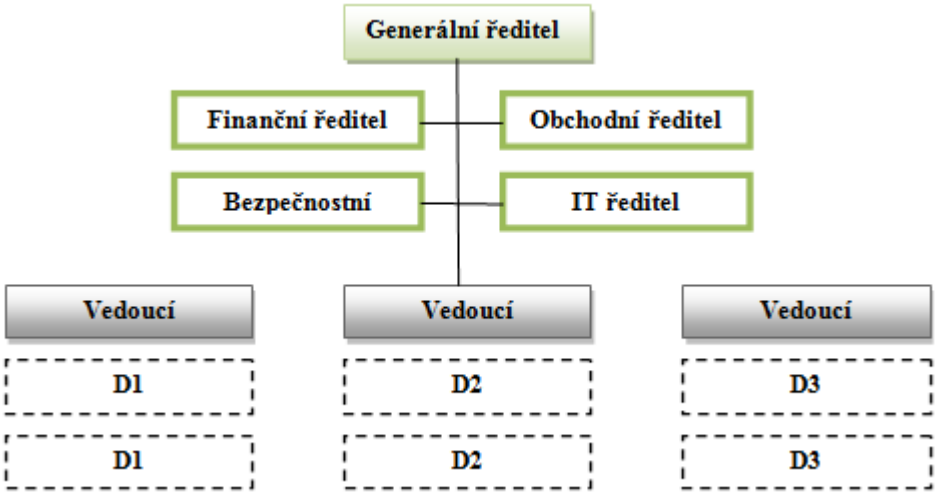
V realizačním projektu uvažuji, že vstup do prvního patra v administrativní budově bude možný buď, pomocí výtahu, nebo pomocí schodiště. Vstup do SW Společnosti by byl možný dvěma vstupy. Hlavní vchod bude přes recepci společnosti, který bude zajištěný systémem pro elektronickou kontrolu vstupu. Dveře půjde otevřít pouze pomocí vstupní karty, kterou bude vlastnit pouze zaměstnanec společnosti. Další způsob otevření vstupních dveří by byl možný pomocí zvonku. Zvonek se umístí u vstupních dveří a řádně označí jménem společnosti. Otevření dveří musí, zajisti pracovník recepce, který bude mít také za úkol danou osobu prověřit, zjistit účel její návštěvy a zapsat údaje o osobě do knihy návštěv.

Druhý vchod do společnosti bude služební vchod, sloužící pouze pro zaměstnance společnosti, dveře budou také zabezpečeny elektronickou kontrolou vstupu a bude možné je otevřít pouze pomocí vstupní karty.

Situaci uvnitř patra navrhuji tak, že kanceláře v prvním patře administrativní budovy budou pronajímatelem standardně vybaveny, zejména kancelářským nábytkem, vybavenou kuchyňkou, kobercem, zdvojenou podlahou pro možnost umístění rozvodů LAN a silnoproudých rozvodů 220V, taktéž budou zajištěné v prostorech, stropní podhledové desky, pro rozvody zabezpečovacích technologií.

Uvnitř společnosti se bude jednat o otevřený prostor s pracovními místy, recepcí, kuchyňkou, toaletou, společným prostorem, kancelářemi, zasedacími místnostmi, dále skladem a servrovnou. Detailnější popis je viz. Obr. 20 Schéma 1. patra SW Společnosti, s.r.o., vnitřní uspořádání firmy.

SW Společnost bude rozčleněná podle organizační struktury společnosti, protože jsou zde zaměstnanci různých odvětví, jako je účetnictví, finance, programátoři, konzultanti, administrativa, IT oddělení a management společnosti.



Obr. 21 Schéma SW Společnosti, s.r.o., organizační struktura

4.4.2 Definice klíčových míst zabezpečení

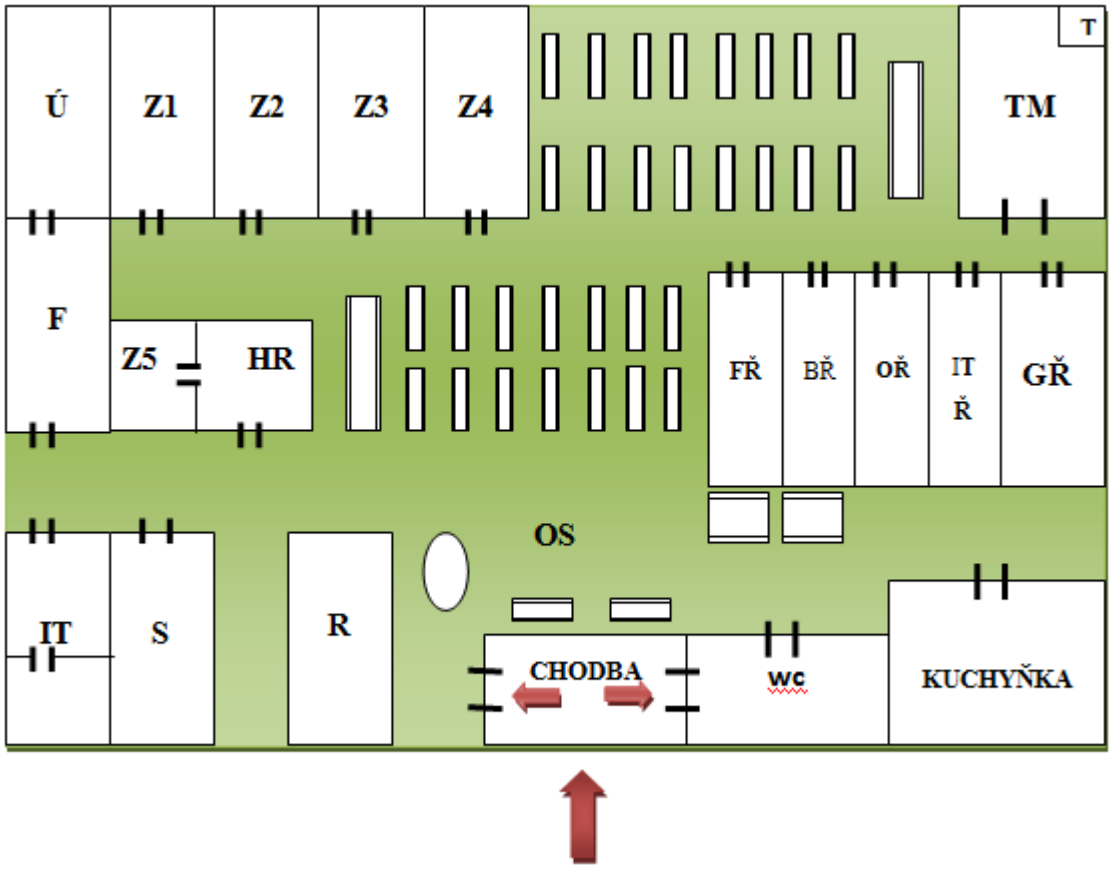
Obecně nejdůležitější místa ve společnosti jsou taková, kde jsou uložena data a kde je umístěna klíčová technologie pro chod společnosti. V našem případě se bude jednat o servrovnu a IT kanceláře a důvěrnou místnost s trezorem. Dále pak místa, kde se s daty pracuje, jako je samostatná uzamykatelná kancelář ředitele SW Společnosti a kanceláře managementu společnosti, personální oddělení a účtárna. A v poslední řadě místa, kde je potřeba dodržovat určitá pravidla, sklad a zasedací místnosti.

Pro všechny místnosti budou navrhované technologie zabezpečení stejné úrovně. Jedinou výjimku tvoří „tajná/důvěrná místnost s trezorem“, která bude popsána a řešena samostatně.

Popis místností v prvním patře administrativní budovy:

- Otevřené kanceláře tzv. open space - (OS)
- Sklad – jeden vstup - (S)
- IT oddělení má celkem 2 místnosti, skládá se z IT místnosti a servrovny. Hlavní vchod je přes oddělení IT a druhý vchod je vstup do servrovny – (IT)
- Finanční oddělení má dva vstupy, jeden hlavní a jeden z oddělení účtárny - (F)
- Účtárna, vstup je možný pouze přes oddělení finanční, tedy dva vstupy – (Ú)
- Personální oddělení má jeden vstup – (HR), je propojeno se zasedací místností, která má jede vstup možný pouze z personálního oddělení - (Z5)
- Zasedací místnost má jeden vstup – (Z1)
- Zasedací místnost má jeden vstup – (Z2)

- Zasedací místnost má jeden vstup – (Z3)
- Zasedací místnost má jeden vstup – (Z4)
- Tajná/důvěrná místnost s trezorem zabezpečená pomocí EZS a EPS, jeden vstup – (TZ)
- Ředitel SW Společnosti, jeden vstup - (GŘ)
- Finanční ředitel, jeden vstup - (FŘ)
- Obchodní ředitel, jeden vstup - (OŘ)
- IT ředitel, jeden vstup - (ITŘ)
- Toalety, dva vstupy – (WC)
- Kuchyňka s jídelnou, jeden vstup - (KJ)
- Recepce je v otevřeném prostoru – (R)



Obr. 22 Schéma 1. patra SW Společnosti, s.r.o., vnitřní uspořádání

4.4.3 Telefonní a datové rozvody, strukturovaná kabeláž

Telefonní a datové rozvody v celém patře musí být umístěny v podlaze a ukončeny na jedné straně v podlahových krabicích pro připojení jednotlivých PC, tiskáren a telefonů, na druhé straně musí být ukončeny v patchpanelu v kabelovém rozvaděči. Musí být použita moderní strukturovaná kabeláž nejméně kategorie 6 splňující přenos 1Gbit. Tento rozvod musí být fyzicky oddělen od strukturované kabeláže budovy a slouží výhradně pro SW Společnost. Tím je omezen přístup a zapojení cizího zařízení do interní sítě. Jediným místem pro přívod Internetu a hlasu je serverovna neboli kabelový rozvaděč, do kterého jsou přivedeny hlasové a datové přípojky operátora. Toto rozhraní musí být zabezpečeno a je řešeno v kapitole Datová a hlasová komunikace popř. Internet a vzdálený přístup.

4.4.4 Elektronický zabezpečovací systém EZS

Systém EZS bude nezávislý od EZS systému budovy. Ústřednu EZS se umístí v serverovně SW Společnosti. Systémem EZS se zastřeží formou detektorů nebo přídavných magnetů a to tato místa, jako hlavní vstupní dveře do patra, vstupní dveře pro zaměstnance, tajná místnost a serverovna. Ochrana bude provedena v důsledku zabezpečení patra po ukončení provozu a odchodu obsluhy.

Signál o narušení by měl být signalizován akusticky, opticky u vstupu do patra sirénou s majákem a rovněž musí být zaveden do centrální recepce budovy. Uvedená rozvodná skříň bude kovová, vhodných rozměrů a chráněná proti neoprávněnému vniknutí tamper kontaktem.

Ústředna EZS je mikroprocesorem řízené programovatelné zařízení sběrnicového typu. Na komunikační sběrnici RS485 budou připojeny jednotlivé komunikační prvky (koncentrátory, klávesnice), které umožňují řízení (klávesnice) a připojení (koncentrátor) vlastních detekčních prvků.

Aktivace a deaktivace systému bude prováděna z klávesnic s nastaveným zpožděním, které jsou umístěny u vstupů do patra. Zabezpečení patra bude navrženo plášťové a prostorové ochrany.

Plášťová ochrana bude provedena magnetickými kontakty na dveřích a oknech. Prostorová ochrana bude ve vnitřních prostorách objektu a bude provedena PIR detektory, které reagují na pohyb osob. Systém by měl umožňovat programovatelné vypnutí některých smyček (při pohybu osob ve vytypovaných místnostech) a zapnutí ostatní signalizace.

Současně by měly být všechny instalované prvky chráněny sabotážní smyčkou, která je trvale v provozu.
Signály od hlásičů a jejich zpracování a vyhodnocení, by měly být přivedeny k ústředně EZS. Veškeré rozvody EZS musí být provedeny dle platných norem.

4.4.5 Systém průmyslové ochrany

V případě kamerového systému pro vnitřní zabezpečení navrhuji instalaci kamerového systému odděleného od CCTV systému budovy. Pro zajištění monitoringu klíčových míst by měly být instalovány spolehlivé kamery propojené koaxiálním kabelem k centrálnímu nahrávacímu zařízení, rekordéru.
Jako klíčová místa monitoringu navrhuji tato:

- Hlavní vstup do patra, kamera bude umístěná nad recepcí, která bude sledovat vstup a prostory před vstupem, protože vstupní dveře jsou prosklené
- Vstup pro zaměstnance, kamera bude umístěná přímo proti těmto dveřím
- Zabezpečená tajná místnost, polokulová kamera s širokým úhlem pohledu pro monitoring prostoru
- Serverovna, polokulová kamera bude sledovat vstup a pohyb osob v serverovně

Kapacita nahrávacího zařízení by měla umožňovat uložení záznamů z těchto kamer minimálně po dobu 7 pracovních dní. Vzhledem k instalaci strukturované kabeláže vyšší kategorie splňující přenos 1Gbitu by bylo vhodné realizovat tento CCTV systém již jako IP systém a využít nových trendů v jednotné kabeláži.
Nahrávacím zařízením by v tomto případě bylo PC/server s CCTV kartou a patřičného software. Samotné dimenzování parametrů není součástí tohoto projektu a mělo by být řešeno v rámci zadávacího/výběrového řízení na tento systém.

4.4.6 Elektronický požární systém EPS

Předpokládám, že má budova, již nainstalovaný robustní systém EPS doporučuji jeho rozšíření v již nastaveném standardu na dané patro s důrazem na klíčové místnosti. Do serverovny navrhuji vybudování stabilního hasicího zařízení SHZ propojeného datově do centrálního požárního systému budovy. Návrh řešení zabezpečení tajné místnosti je řešený v další kapitole. V rámci administrativních náležitostí musí být vypracovány dokumenty popisující stavy těchto systému a postupy řešení událostí.

4.4.7 Elektronická kontrola vstupu EKV (ACS)

Pro zajištění přístupu do patra a předem definovaných klíčových míst zabezpečení navrhuji instalaci nového, nezávislého systému zabezpečení. Vzhledem k již nainstalovanému EKV systému budovy a propojení na vstupy do patra (hlavní vstup, vstup pro zaměstnance) doporučuji využití stejné technologie přístupových karet jako má EKV systém budovy. Značně se tím zjednoduší evidence karet a jejich přidělování, včetně řešení případných ztrát. Každý pracovník dostane přidělenu kartu přístupového systému a bude zaveden do software obsluhující EKV systém. Tento centrální PC/server je umístěný v serverovně SW Společnosti a sběrnicově připojuje dvě navrhované jednotky přístupového systému, které jsou každá dále členěny na dvě čtečky u každých výše definovaných dveří. Výstup z těchto místností bude realizován klikou kromě tajné místnosti. Pomocí nasazení systému EKV dojde k předem definovanému pohybu osob. Celé toto řešení musí být doplněno o prostředky administrativy, které jsou definovány v dalších kapitolách.

4.4.8 Detailní návrh zabezpečení tajné místnosti

- **Režim činnosti systémů v případě, že je místnost zastřežena**

Oprávněná osoba přiloží kartu ke čtečce a zadá kód pro odstřežení místnosti. Systém zpřístupní místnost, zhasne kontrolní dioda a odemkne se zámek. Osoba vstoupí do místnosti a bude zaevidován průchod osoby. Současně s tím bude zaevidována do systému ANTIPASBACK.

Další možný návrh zastřežení vstupu do tajné místnosti může být způsobem takovým, že pokud do stanoveného času, osoba nevstoupí do místnosti, bude proveden záznam do systému a místnost se opět zastřeží a rozsvítí se kontrolní dioda (cca 10 s). Vejde-li další osoba do místnosti, bude zaevidován její průchod a osoba bude zaevidována do systému ANTIPASBACK.

- **Režim činnosti systémů v případě, že je místnost odstřežena**

Oprávněná osoba přiloží kartu ke čtečce a zadá kód pro odstřežení místnosti. Systém odemkne zámek. Osoba odejde z místnosti, přičemž bude zaevidován průchod a osoba bude odečtena ze systému ANTIPASBACK. Pokud se jedná o poslední osobu v systému ANTIPASBACK dojde po uzavření dveří k zastřežení místnosti a rozsvícení diody.

Další možný návrh zastřežení výstupu do tajné místnosti může být nadefinovaný tímto způsobem, pokud se nejedná o poslední osobu v místnosti, bude pouze zaevidován

průchod. Pokud jsou dveře otevřeny jiným způsobem (klíčem nebo násilím) dojde k vyhlášení poplachu a odeslání varovné zprávy pomocí GSM komunikátoru.

4.4.9 Technické řešení vnitřního zabezpečení tajné místnosti v prvním patře administrativní budovy

- **Systém EZS**

Systém EZS bude v "zabezpečené oblasti" instalován v rozsahu prostorové, plné plášťové ochrany a tísňového tlačítka. EZS "zabezpečené oblasti" bude řešený, jako samostatný nezávislý podsystém. Jádrem systému je ústředna společnosti. Mělo by se jednat o ústřednu „sběrnicového typu“, kdy na sběrnici ústředny jsou připojeny komunikační moduly (expandéry, klávesnice apod.) Uvedené moduly vytvářejí bezpečnostní podsystémy a jejich umístění není závislé na vlastním umístění ústředny EZS. Na komunikační sběrnici by měly být připojeny jednotlivé komunikační prvky (koncentrátory, klávesnice), které umožňují řízení (klávesnice) a připojení (koncentrátor) vlastních detekčních prvků.

Aktivace a deaktivace systému bude prováděna z klávesnice s nastaveným zpožděním, která je umístěna u vstupu do místnosti (společná klávesnice systémů EZS a EKV).

Zabezpečení objektu je navrženo plášťové a prostorové. Plášťová ochrana bude provedena magnetickými kontakty na dveřích a oknech. Prostorová ochrana bude navržena ve vnitřním prostoru místnosti a bude provedena PIR detektorem a detektorem tříštění skla.

Systém umožňuje programovatelné vypnutí některých smyček při pohybu osob. Současně budou všechny instalované prvky chráněny sabotážní smyčkou, která bude trvale v provozu. Na systém EZS bude připojen opticko-kouřový detektor požáru pro vyhodnocení požárního nebezpečí.

Signály od hlásičů a jejich zpracování a vyhodnocení, budou přivedeny k ústředně EZS. Následně podle naprogramovaných reakcí výstupů bude taktéž aktivován komunikátor GSM, který bude umístěn ve stejné místnosti jako ústředna systému. Veškeré rozvody EZS musí být provedeny dle platných norem.

Expandéry (2ks) EZS musí být umístěny v "objektu", v místnosti. Výstup hlášení poplachových stavů jednotlivých prvků EZS instalovaných v "zabezpečené oblasti" by měl být vyveden prostřednictvím expandérů a komunikační sběrnice do klávesnice EZS instalované na stanovišti fyzické ostrahy v centrální recepci budovy, a zároveň bude poplachový signál z ústředny EZS bezdrátově přenášen (komunikátor GSM) na mobilní

telefon odpovědného pracovníka společnosti nebo příslušníka ostrahy provádějícího obchůzku.

Klávesnice EZS/EKV (společná) je určená k aktivaci a deaktivaci EZS "zabezpečené oblasti" (současně s ověřením platné bezkontaktní karty) měla by být instalována u vstupních dveří do "zabezpečené oblasti".

V "zabezpečené oblasti"by měly být instalovány tyto prvky EZS:

- Prostorový PIR/MW detektor
- Detektor tříštění skla
- Tísňový hlásič
- Magnetické kontakty (dveře, okno)
- Opticko-kouřový požární hlásič

- **Systém EKV**

V "zabezpečené oblasti“ by měl být realizován systém EKV. Centrální řídící jednotka systému EKV by měla být umístěna v serverovně SW Společnosti. Tato řídící jednotka by měla být datově propojena s řídící ústřednou EZS, současně by měla být propojena do datové sítě (propojení na řídící/datový server) a také na jednotku dveřního modulu (interface) v tajné místnosti. Na tento dveřní modul by měly být připojeny dvě čtečky bezkontaktních karet, obě v provedení „s klávesnicí“. Jedna by měla být instalována vně „zabezpečené oblasti“ a druhá uvnitř „zabezpečené oblasti“. Dveřní jednotka (interface) svým výstupem ovládá elektromechanický zámek bezpečnostních dveří místnosti.

Vzájemné programové vazby systému EKV na systém EZS budou provedeny datovým spojením (propojovací kabel) na úrovni propojení ústředny EZS a řídící jednotky EKV.

Elektrický systém kontroly vstupu bude tedy ovládán kartou. Přečtením platné karty systému a zadáním správného bezpečnostního kódu na klávesnici u vstupu dojde k uvedení bezpečnostního prostoru tajné místnosti do stavu odstřežení a následnému otevření zámku dveří.

Uvedený stav odstřeženo nebo zastřeženo bude signalizován optickou signalizací nad vstupními dveřmi do tajné místnosti. Po odchodu oprávněného pracovníka z místnosti a přečtením karty včetně zadání kódu bude systém automaticky uveden do režimu střežení.

V rámci administrativních náležitostí je vhodné vypracovat dokumenty popisující práci, oprávnění a další s tím spojené postupy pro nastavení správného provozu této místnosti.

4.5 Zajištění vnitřní bezpečnosti na úrovni systémů a práce SW Společnosti

Administrativní budova má již navržený systém vnějšího zabezpečení a vnitřní zabezpečení na úrovni prvního patra. V následující kapitole budou navrženy možné způsoby zabezpečení se zaměřením na vnitřní bezpečnost společnosti. Předpokládám, že SW Společnost není certifikovaná.

Za bezpečnost informačních a komunikačních technologií ve vztahu k informacím a informačním systémům musí zodpovídat z pověření ředitele společnosti definovaný pracovník.

Jako místnost s vysokou koncentrací ICT je předem definována serverovna SW Společnosti. Pro místnosti s vysokou koncentrací ICT musí být zajištěno fyzické oddělení od ostatních provozních aktivit a kontrola přístupu průchodu uzamčenými dveřmi vyžadujícími pro otevření speciální klíče. Identifikační předměty nebo kódy musí být předány pouze určeným osobám. Přístup může mít pouze autorizovaný personál a všechny činnosti musí být zaznamenávány. Umístění v objektu, jehož zdi, stropy a podlahy mají konstrukci a prvky zpomalující hoření. Dveře se zajištěním proti násilnému vstupu. Zajištění požární bezpečnosti nejméně v rozsahu, daném vyhláškou pro prostory se zvýšeným požárním nebezpečím, zařízení ICT musí být chráněno proti všem formám poškození vodou, parami nebo extrémní vlhkostí, prostory musí být odděleny od obslužných oblastí, jako například pro nakládku a vykládku.

Zařízení ICT s výjimkou uživatelských koncových stanic, musí být umístěna v tzv. místnostech s vysokou koncentrací ICT - serverovně a musí být správně udržována podle dokumentace výrobce nebo dodavatele. Pro počítačové zařízení, klimatizaci a bezpečnostní systémy musí být zabezpečeno spolehlivé elektrické napájení bez poklesů a špiček, zabezpečené podle potřeby záložními zdroji, záložní zdroj energie by měl pracovat v reálném čase a musí být testován podle pokynů výrobce. V prostorách se zvýšenou koncentrací ICT musí být instalováno samočinné nouzové osvětlení, které je aktivováno v případě výpadku napájení. Napěťové a komunikační kabely musí být oddělené od ostatních služeb, aby nemohlo dojít k útoku na data touto cestou, průchody kabeláže zdmi nebo stropy nesmí snižovat stávající požární ochranu, zařízení s instalovanou ochranou proti blesku, klimatizační systém se zařízením pro monitorování funkce, zařízení s možností uchovávání informací musí být spravována mimo dohled SW Společnosti,

zařízení ICT musí podléhat evidenci a změna jeho umístění se musí provádět jen se souhlasem vlastníka.

4.5.1 Popis současného stavu ICT systémů SW Společnosti

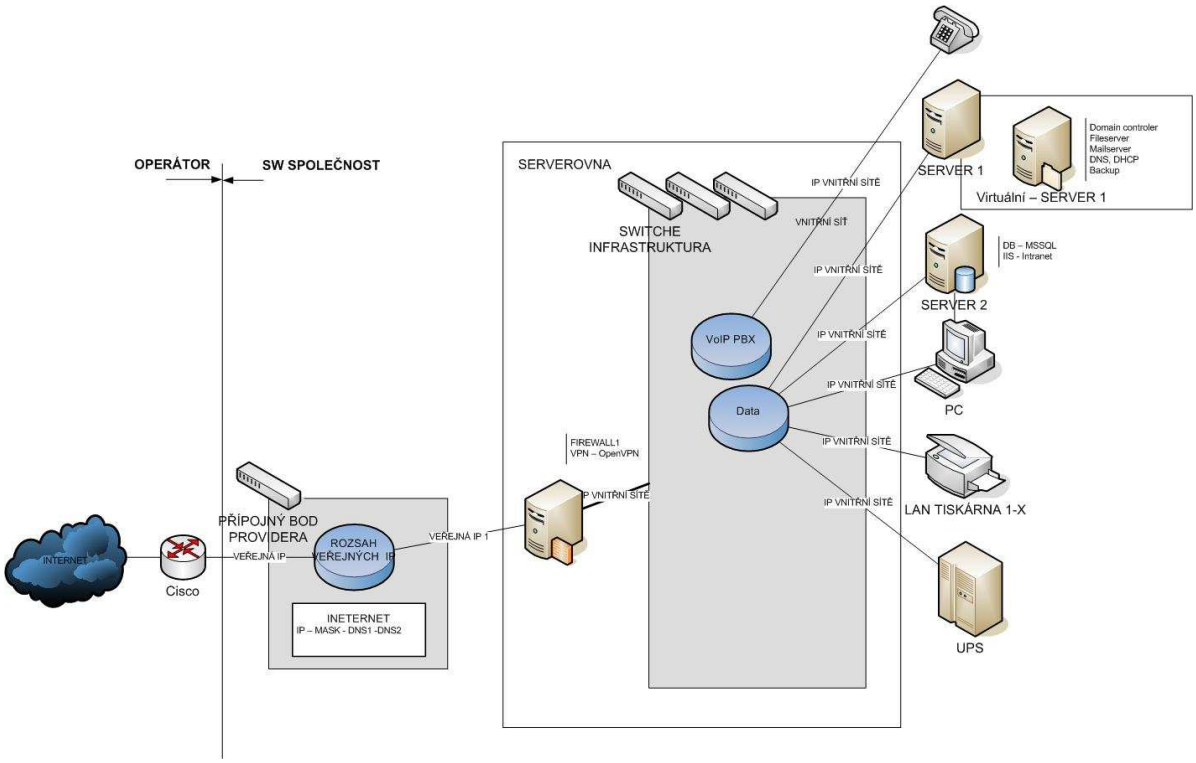
Popis současného stavu ICT systémů SW Společnosti před nastěhováním do nových prostor.

Současná infrastruktura „před stěhováním“ se skládá z jednoho staršího serveru plnící úlohu datového úložiště bez možnosti pravidelného zálohování a jeden standardní PC sloužící jako Firewall a poštovní server. Je využíván starší typ strukturované kabeláže kategorie 5e. Telefony jsou řešeny na úrovni budovy s připojením do analogové ústředny budovy. Další infrastrukturu tvoří samotné počítače uživatelů, černobílé tiskárny v počtu 2ks připojené do LAN a jedné barevné tiskárny připojené přímo k PC. Telefony jsou standardní analogové připojené na základě starší dvojlinkové kabeláže k ústředně budovy, celkem 15 klapek. Není zaveden jednotný systém přístupu k datům a není řešeno zálohování.

4.5.2 Návrh změny uspořádání ICT systémů

Infrastruktura by se měla skládat ze čtyř hlavních částí. Hardware, operační systém, poštovní server a bezpečnostní software. Jako hardware by měl být zvolen robustní server, dostatečně paměťově a prostorově dimenzovaný s možností rozšíření (vizualizace jako nástroj pro další expanzi sužeb a využití maximálního výkonu serveru) s platnou servisní smlouvou (SLA), nejlépe 4 hodin opravou na místě, aby nedošlo k ohrožení práce společnosti jako celku. Operační systém bude Microsoft Windows SBS Server s integrovaným poštovním server MS Exchange 2003. Bezpečnostní SW například od firem ESET (antivir) a Gfi (antivir a antispam). Firewall s platnou smlouvou pro aktualizace zabezpečení, nejlépe „appliance“ sloužící přímo k dané činnosti, aby bylo znemožněno komukoliv přístupu do vnitřní sítě SW Společnosti. Výše zmíněné části tvoří klíčové oblasti zabezpečení. Tyto části musí být umístěny v serverovně SW Společnosti, odborně zabezpečeny na úrovni operačního systému a aplikační vrstvy. K dalšímu klíčovému hardware by měla být IP telefonní ústředna pro zajištění moderní hlasové a video komunikace, jak po LAN, tak i přes Internet. Vzhledem k činnosti firmy je důležitá implementace jednotného způsobu automatického zálohování dat na serveru s využitím např. páskových zálohovacích jednotek dostatečné kapacity odpovídající diskovému prostoru serveru.

Jako centrální aktivní prvek zajišťující komunikaci uvnitř sítě LAN je potřeba naimplementovat robustní managovatelný switch s dostatečným počtem portů splňující požadovanou rychlost komunikace sítě. Dále je vhodné využít standardních switchů a propojit je do jednoho celku. Hlavní switch musí sloužit pro připojení náročných technologií typu server, „podružné“ switche pak musí sloužit k připojení jednotlivých PC a tiskáren a podobně.



Obr. 23 Schéma, návrh LAN, po stěhování společnosti

4.5.3 Umístnění klíčových technologií

Všechny klíčové technologie (server, IP telefonní ústředna, zálohování) musí být umístěny centrálně a to v místě s vysokou koncentrací ICT, tedy v serverovně SW Společnosti. Jedině, tak lze definovat oprávnění pro fyzický přístup k nim. Do serverovny by měl mít přístup pouze pověřený, odborně způsobilý pracovník.

4.5.4 Návrh řešení zabezpečení oblastí

Bezpečnost je rozdělena do dvou skupin. První je bezpečnost dat jednotlivých uživatelů proti neoprávněnému přístupu a druhou je zabezpečení počítačů a celé sítě proti virovým a jiným útokům.

Bezpečnost dat v lokální síti musí být řešena nutností přihlášení k doménovému serveru. Přístup k datům z prostředí internetu je navíc doplněn o zabezpečení SSL.

Všechny prostředky ICT, jichž se to týká, musejí mít instalován prostředek na ochranu před nebezpečnými programy a kódy. Tyto prostředky musí být udržovány ve spolehlivém a aktuálním stavu. Instalace a přístupová práva k prostředkům ICT musí být nastavena tak, aby prostředek na ochranu před nebezpečnými programy a kódy mohl odstavit či vypnout jen ten pracovník, který provedl jeho instalaci.

U mobilních zařízení, která nejsou trvale připojena k síti SW Společnosti, musí být zajištěno, že se aktualizace prostředku na ochranu před nebezpečnými programy a kódy provede při každém připojení k síti společnosti. Aktualizace se zajistí, jako služba nebo jako první operace po identifikaci a autentizace uživatele.

Bezpečnost sítě musí být řešena nasazením několika produktů, které se vzájemně doplňují. Především je to nasazení souborového antivirového software na stanice a servery. Zabezpečení poštovního serveru musí být řešeno odpovídajícím produktem, který v základu obsahuje alespoň dvě antivirová jádra a to pro větší bezpečnost. Všechno musí být doplněno o ochranu před nevyžádanou poštou.

V neposlední řadě je nutné zajistit nasazení služby Windows Software Update Services pro centrální správu aktualizací operačního systému a ostatních aplikací Microsoft v celé síti.

4.5.5 Datová a hlasová komunikace

Bezpečnost sítě SW Společnosti musí být konstruována tak, aby umožňovala přístup zaměstnanců a třetích stran v rozsahu, který odpovídá jejich pracovnímu zařazení. Zvláštní předpis musí být vydán pro práci mobilních zařízení. Konfigurace sítě musí být chráněna proti neoprávněnému zásahu. Musí být zajištěno, aby byly zprávy vysílány pouze z výstupního uzlu do cílového uzlu.

Výměna informací mezi zaměstnanci společnosti nebo třetími stranami, musí být řízena v rámci definovaných pravidel. Informace nesmí být zasílány elektronickou poštou nebo podobnými veřejnými kanály bez předchozího zašifrování spolehlivým algoritmem.

Hlasová komunikace musí být řešena moderně s využitím technologie IP zajišťující zabezpečenou a šifrovanou komunikaci. Zajištění telefonních stanic před neoprávněným požitím musí být zajištěno na úrovni hesla a pinu.

4.5.6 Internet, vzdálený přístup

Vzdálený přístup k datům by měl být řešen přes certifikovanou a vysoce zabezpečenou VPN.

Veškerá poštovní korespondence musí být přesunuta na Exchange server. Tento server musí být nastaven jako primární poštovní server klienta. Pro přístup k mailům lze použít lokálně MS Outlook nebo pro vzdálený přístup rozhraní Outlook Web Access se zabezpečením SSL. Měla by být zprovozněna služba faxového serveru a veškerá faxová korespondence převedena z papírové do elektronické podoby. Jediná a tím centrální přípojka k Internetu musí být přivedena do kabelové rozvaděče umístěného v serverovně.

4.5.7 Hardware

Všechny servery, telefonní ústředna i zabezpečovací systémy musí být napojeny na inteligentní záložní zdroje UPS. Návrh řešení infrastruktury hardware je řešena v kapitole 4.5.2. Návrh změny uspořádání a propojení ICT systémů.

V případě, že je nutné předat pevné disky z počítačů, servrů nebo jiných médií, musí platit přísná bezpečnostní opatření. Odpovědná osoba musí předat do opravy pouze média, která jsou vymazaná a zformátovaná, aby nedošlo k nežádoucímu úniku informací. V případě, že tímto způsobem nelze zabezpečit média, tak se akceptuje skartace.

4.5.8 Zálohování a archivace dat

Pro případ neodborné manipulace s daty je důležité zajistit pravidelné zálohování dat, souborů, vytvořením bezpečnostních kopií na média tomu určená, jako například CD, DVD, a další. Zálohované data můžeme využít v případě nečekané havárie k obnově datové základny.

V rámci bezpečnosti zálohy, je nutné citlivá data ukládat do firemního trezoru, který je umístěný v uzamykatelné místnosti a mají k němu přístup pouze určené osoby. Kopie se provádí dle potřeby avšak s určitou pravidelností. Zálohování by se mělo provádět ve dvou vyhotoveních.

Archivaci navrhuji provádět 1x ročně ve dvou vyhotoveních. Archivaci provádí vždy určená osoba. Archivní media je nutné dobře označit (rok/datum/citlivost údajů, popřípadě další potřebné údaje). Archivace se doporučuje provádět ve dvou vyhotoveních, jedno vyhotovení slouží pro úschovu v trezoru společnosti a druhé vyhotovení je možné uschovat například v bance.

Pro práci s informacemi na počítačově čitelných médiích musí být zajištěno, že kvalita médií odpovídá účelu, pro který jsou pořizována a to bez ohledu na nákupní cenu, uskladňování médií před jejich uvedením do používání musí odpovídat pokynům dodavatele, výrobce, každé médium, sloužící pro trvalé zpracování dat, musí být označeno a evidováno. Média musí být likvidována podle stupně ochrany informací na nich uložených. Skladům médií nositelů dat s daty určenými pro obnovu po havárii musí být věnována zvláštní péče. Uložení médií musí být provedeno v souladu se zvláštním předpisem.

Papírové doklady, tedy informace, v papírové podobě, které vznikají ve společnosti, mohou být uloženy v kancelářích nebo v archivu společnosti. K zamezení zneužití dokumentů z bezpečnostního hlediska se doporučuje skartace chybných nebo už nepotřebných dokumentů. Za skartaci dokumentů vždy odpovídá příslušná osoba z oblasti bezpečnosti. Skartaci dokumentů je možné provádět i externě, tedy externí společností za určitých podmínek, dodavatel skartací musí mít zavedený a certifikovaný systém dle platných norem.

4.5.9 Software

Programové prostředky ve spolupráci se síťovým hardware zajišťují činnost sítě.

SW Společnost používá ve svých PC a serveru operační systém Windows. V rámci bezpečnosti a uchování dat musí být do každého PC nainstalován antivirový program, který slouží pro kontrolu či odhalení zavirovaných souborů. Tento antivirový program se spustí zároveň se spuštěním PC či serveru. Uživatelé PC by neměli mít právo zasahovat do konfigurace antivirového programu. Možnost změn či aktualizaci antivirového programu, může pouze stanovený pracovník IT oddělení.

Pro každý IS musí jeho majitel, správce stanovit minimální bezpečnostní požadavky. Pokud je to možné, musí se na zpracování těchto požadavků podílet bezpečnostní specialista.

Musí být zavedena evidence licencovaného software, jeho aktualita a ochrana před neoprávněným kopírováním tj., uložením v trezoru SW Společnosti.

4.5.10 Administrativa bezpečnosti

Za administrativní bezpečnost vzhledem k informacím a informačním systémům musí být určená zodpovědná osoba, která bude zodpovědná za administrativní bezpečnost společnosti.

Společnost musí také určit a definovat ve svých dokumentech, zda se jedná o informace veřejné, neveřejné nebo informace jen pro potřeby SW Společnosti.

Vedení SW Společnosti je odpovědné za své zaměstnance ve smyslu bezpečnosti informací.

- **Personální bezpečnost**

Za personální bezpečnost ve vztahu k informacím a informačním systémům, musí být určená odpovědná osoba v oblasti personální bezpečnosti. Musí být správně nadefinované pravomoci a odpovědnosti zaměstnance tak, aby měl přístup pouze k činnostem v informačním systému, které odpovídají jeho pracovnímu zařazení. Zaměstnanec, který má přístup k důležitým informacím musí podepsat příslušný dokument o hmotné zodpovědnosti a projít patřičným školením.

- Povinnosti zaměstnance

Každý zaměstnanec společnosti musí být seznámen se zásadami bezpečnosti informací o pravomocech při zpracování informací. Pak je zaměstnanec povinen stanovené zásady dodržovat. Zaměstnancům musí být umožněný přístup k bezpečnostním pravidlům společnosti, aby měli možnost kdykoliv podle jejich potřeby do dokumentu nahlédnout.

Personální bezpečnost můžeme rozdělit do několika etap podle období, ve kterém se zaměstnanec právě nachází. Jedná se zejména o období nástupu zaměstnance do společnosti, kde by měl projít vstupním pohovorem se svým nadřízeným pracovníkem, dále přidělení pracovní role a definice zodpovědnosti i bezpečnostní zodpovědnosti a předání pracovní smlouvy.

V průběhu trvání pracovně právního vztahu, se zaměstnancem se mu přidělí oprávnění k manipulaci s informacemi, podle zařazení jeho pracovní pozice. Jsou mu přidělena práva a hesla potřebná k vykonávání pracovní činnosti. Zaměstnanec podle zařazení pracovní pozice by měl projít potřebnými školeními, která budou zaměřené na bezpečnost a ochranu informací.

V případě, že zaměstnanec změní pracovní pozici v rámci společnosti, musí mu být realizovaná změna nebo i zrušení patřičných oprávnění, přístupů, hesel a dalších identifikátorů. V případě ukončení pracovního poměru se zaměstnancem je nezbytné z bezpečnostního hlediska odebrat uživateli veškerá přístupová práva do systému a ukončit manipulaci s informacemi ve společnosti. Dále je povinností zaměstnance odevzdat pracovní prostředky, které měl k vykonávání pracovní činnosti ve společnosti.

Společnost by měla zajistit pro své zaměstnance pravidelná školení o bezpečnostní zodpovědnosti, tak aby znali své povinnosti a byli si plně vědomi, že informace ve společnosti jsou věcí neveřejnou. Při porušení zásad bezpečnosti, jako například při neoprávněném nakládání s informacemi, musí proběhnout šetření se zaměstnancem a stanovit důsledky, podle výsledků šetření.

Objekt společnosti musí být po dobu pracovní doby střežen pracovníky recepce, kteří jsou zodpovědní za pohyb nepovolaných osob v objektu společnosti. Po pracovní době bude objekt uzamčen a zajištěn alarmem, který je napojený na bezpečnostní službu.

Na recepci společnosti bude i centrála pro úschovu klíčů, které společnost vlastní. Klíče budou uložené v uzamykatelné skříňce a jejich zapůjčení evidují pracovníci recepce, kteří se zároveň starají o jejich bezpečnost.

- **Bezpečné chování uživatelů ve společnosti**

Z bezpečnostního hlediska má mít každý zaměstnanec společnosti přiřazený jeden účet do informačního systému. V počítačové síti je pak zaměstnanec identifikován svým účtem v operačním systému. Přihlášení k těmto účtům jsou chráněna heslem. Přístupová práva jsou zaměstnanci přidělena na základě pracovního zařazení. Pověřená osoba IT oddělení provádí přidělování práv jednotlivým zaměstnancům dle stanovených kritérií společnosti. Ke změnám přístupových práv se přistupuje, jako ke zrušení dosavadních práv a založení nových přístupových práv. O zrušení přístupových práv zaměstnanci rozhoduje nadřízený pracovník nebo osoba odpovědná. K zrušení práv musí dojít při ukončení pracovního poměru zaměstnance.

Každý zaměstnanec SW Společnosti je povinen se chovat ve společnosti tak, aby nedocházelo k úniku informací v papírové, elektronické či jiné podobě. V případě, že zaměstnanec opouští své pracovní místo, tak bude povinen provést několik základních kroků, které vedou k zabezpečení pracovního místa. Jedná se o odhlášení počítače ze systému, uklizení pracovní plochy tak, aby na stole nezůstaly citlivé dokumenty, jako jsou smlouvy, diskety a jiné materiály, které by mohly způsobit ztrátu informací a nedošlo tak k jejich případnému zneužití.

Na základě požadavku od nadřízeného pracovníka bude novému zaměstnanci v SW Společnosti, zřízena e-mailová schránka na e-mailovém serveru a to odpovědným pracovníkem IT oddělení. Zaměstnanec společnosti musí dbát, aby prostřednictvím e-mailu nedošlo k úniku informací. Musí dbát na to, aby informace, které se prostřednictvím e-mailu posílají, byly správně adresované, musí kontrolovat správnost příloh, které zasílají,

dále nesmí sdělovat žádné interní záležitosti. Každý zaměstnanec společnosti bude zodpovědný za veškeré data a informace, které odešle prostřednictvím e-mailu. Zaměstnanec bude dále zodpovědný za pravidelné zálohování došlé pošty v e-mailové schránce.

Elektronický podpis bude aplikován podle požadavků společnosti, které tento podpis vyžadují.

- **Fyzická bezpečnost**

Za fyzickou bezpečnost ve vztahu k informacím a informačním systémům, musí být určená odpovědná osoba v oblasti fyzické bezpečnosti.

Bezpečnost přístupu do objektu kanceláří se musí řídit pravidly pro zajištění bezpečnosti SW Společnosti jako celku.

Vstup do objektu kanceláří je přes recepci společnosti. Vstupuje-li do objektu návštěva, která se bude pohybovat po objektu SW Společnosti, musí pracovník recepce zapsat údaje o návštěvě do knihy návštěv. Jedná se zejména o jméno osoby, firma a účel návštěvy. Návštěva musí podepsat dokument, ve kterém stvrzuje, že se bude chovat podle nadefinovaných pokynů zaměstnance, který ho bude po SW Společnosti doprovázet a tím i převezme za něho zodpovědnost. Návštěva nesmí bez souhlasu pověřené osoby připojovat soukromé PC k síti LAN společnosti, dále ji musí být zamezený přístup do interní sítě společnosti.

- **Přiřazení odpovědností**

Základní přiřazení odpovědností ve společnosti musí být nadefinované a zřejmé, včetně odpovědnosti za majetek a procesy spojené z bezpečností informací.

Přiřazení odpovědností bude také dáno osobní odpovědností zaměstnance, a to podpisem dokumentů, ve kterých se specifikuje náplň práce, přiřazení role, hmotná odpovědnost za majetek i informace a zachování důvěrnosti ke společnosti.

5 NÁVRH VHODNÝCH OPATŘENÍ, KTERÁ POVEDOU KE ZVÝŠENÍ BEZPEČNOSTI, KONKURENCESCHPNOSTI A RŮSTU SPOLEČNOSTI

Vzhledem k tomu, že SW Společnost získala zakázku velkého rozsahu pro státní správu a bude disponovat zvýšeným počtem zaměstnanců a širokým rozsahem poskytovaných služeb s velkým množstvím dat a informací bude z mého pohledu nezbytná certifikace společnosti renomovanou certifikační autoritou, tedy externí společností.

5.1 Návrh vhodných opatření pro SW Společnost

Výhodou certifikované společnosti je zvýšení důvěryhodnosti, zlepšení ochrany dat a bezpečnosti informací, získání patřičného image v postavení na trhu a růstu konkurenceschopnosti. Společnost tímto poskytne svým zákazníkům nebo partnerům důkaz o tom, že uplatňuje v rámci bezpečnosti informačních a komunikačních systémů důvěryhodné a certifikované postupy.

Optimální varianta se tedy jeví příprava bezpečnostní politiky při účasti externí firmy za předpokladu, že do pracovního týmu externí společnosti budou začleněni i pracovníci SW Společnosti. Výhodou pak je, že zaměstnanci převezmou potřebné znalosti a podklady pro údržbu a rozvoj. Obsah bezpečnostní politiky musí zahrnovat veškeré aspekty zabezpečení ochrany organizace proti všem hrozbám, interního a externího původu, jako např. zabezpečení administrativní budovy, bezpečnost zaměstnanců, archivaci a zálohu dat až po plán obnovy. Bezpečnostní politiku ve společnosti schvaluje vedení organizace. Po schválení je závazná pro všechny zaměstnance.

Dalším aspektem, který povede k růstu společnosti je konsolidace informačních systémů a co nejvyšší možná míra integrace uvnitř společnosti. Nastavení jednotného systému předávání a zpracování informací mezi jednotlivými odděleními, ale i komplexní informační komunikace. Cílem musí být zamezení neefektivnosti a odstranění duplicit, to znamená mít informace ve srozumitelné podobě na všech stupních řízení, jako operativní, dílčí, sumární, v podobě statistik a plánování.

5.2 Zvýšení konkurenceschopnosti SW Společnosti

Ke zvýšení konkurenceschopnosti společnosti přispěje inovace vzdělávacího systému. Je známo, že zaměstnanci, tedy uživatelé ICT představují vážnou hrozbu pro bezpečnost společnosti. Zaměstnancům musí být umožněny různé druhy vzdělávání, které vedou

k vyšší produktivitě a profesionalitě při práci, ke zlepšení komunikace uvnitř i vně společnosti. Vyšší kvalifikací zaměstnanců dojde k posílení pozice společnosti na trhu. Dosažením vyšší kvality poskytovaných služeb se zvýší pravděpodobnost, že uspěje před konkurencí.

5.3 Shrnutí

V současném, rychle se rozvíjejícím světě je nezbytně nutné sledovat vývoj jednotlivých oblastí, pružně reagovat na změny a zajistit si tak silnou pozici na trhu.
Tato pozice ale vyžaduje nemalé investice a pružnost v celé šíři činností společnosti.
Některá opatření, která vedou ke stabilitě a růstu společnosti jsou například průběžným sledování vývoje technologií a trendů, poskytováním vzdělávání zaměstnancům, dodávkou kvalitních služeb, servisu a záruky, referencemi, aktualizací bezpečnostní dokumentace, certifikací, efektivností, ekonomikou a správným financováním společnosti.
Při výběru opatření je možné se řídit přílohou A normy ČSN ISO/IEC 27001:2006

ZÁVĚR

Bezpečnost IT se stala jedním z nejdůležitějších oborů informačních a komunikačních technologií. V dnešní době ji ovlivňují nejnovější technologie a produkty, prosazované v rámci ICT, které vytvořily prostředí měnící se podle požadavků, vývoje a znalostí v různých oblastech bezpečnosti. Společnost, firma či organizace si musí umět ochránit své strategické informace, zajistit si důvěryhodnost a účelně umět investovat do zabezpečení informačního systému i ochrany společnosti.

Oblast bezpečnosti informačních a komunikačních technologií se neustále vyvíjí a neustále na trh přicházejí nové trendy. Většina společností, která působí v oblasti informačních systémů, využívá běžně dostupné produkty ke svojí každodenní činnosti. Bezpečnost ICT systémů však nemůže být uživatelům podrobně známa a ve většině případů se musí spoléhat na dodavatele, že zajistí potřebné bezpečnostní opatření a tím i kvalitu používání informačních systémů ve společnosti. Odpovědní vlastníci informačních systémů musí tedy řídit rizika spojená s jejich používáním. Musí mít všeobecný přehled o trendech a výborně se orientovat na trhu tak, aby uměli pružně reagovat na případné bezpečnostní hrozby. Moderní společnost si v dnešní době musí umět obhájit důležitost informační bezpečnosti a případné investice do jejího zlepšování chápat, jako druh pojištění před případnými hrozbami v daném informačním systému.

Teoretická část diplomové práce souhrnně popisuje současné možnosti zabezpečení a ukazuje cesty k případným zlepšením. Dává jasný pohled na problematiku a umožňuje v celém komplexním oboru bezpečnosti ICT se zorientovat. Praktická část, pak dává návody, jak postupovat a co neopomenout při případné realizaci a je koncipována, jako realizační projekt vnitřního i vnějšího zabezpečení softwarové společnosti.

Práce je přínosná pro menší společnosti stejného nebo podobného charakteru v oblasti zabezpečení ICT, které se chystají expandovat a budou muset přemýšlet o efektivním zabezpečení společnosti jako celku. Vnitřní zabezpečení společnosti na úrovni systémů je konkrétně řešena pro společnost Comapactive, s.r.o., pro zefektivnění jejího vnitřního chodu a využití pro další realizační projekty zabezpečení budov a firem.

CONCLUSION

IT security has become one of the most important fields of information and communication technologies. Today it is affected by the latest technology and products, promoting the ICT, which developed according to changing requirements, developments and knowledge in various areas of security. Company, firm or organization must be able to protect its strategic information, to secure the credibility and know how to effectively invest in information system security and protection of society.

The field of the security of information and communication technologies is all the time in development and new trends are coming on the market. Most of the companies being active in the information system field are using currently accessible products for their everyday activity. But the security of the ICT systems can not be known to the users in detail and in the most of the cases they must rely at the supplier that he will ensure the necessary security measures and by this also the quality of using of the information systems in the society. The responsible proprietors of the information systems must therefore control the risks connected with their use. They must have a general overlook about the trends and to orient themselves very good at the market, so that they could lively react at the eventual security menaces. A modern society has, in this time, to know, how to state its case of the information security importance and to comprehend eventual investments to its improvement as a kind of insurance against eventual menaces in the given information system.

The theoretical part shows complexly the contemporary possibilities of the safeguard and the ways to eventual improvements, as well. It gives a clear view at the problematic and makes possible to be oriented in the whole complex field of the ICT security. The practical part is giving then the guidance, how to proceed and what should not be forgotten during the eventual realization. It is drawn as a realization project of both, internal and external safeguarding of the software society. Work is beneficial for smaller companies the same or similar nature in the field of ICT security, which plan to expand and will have to think about the effective security of society as a whole. Internal Security systems level is a specific solution for the company Comapactive, s.r.o., to streamline its internal functioning and utilization of other implementation projects for buildings and businesses.

SEZNAM POUŽITÉ LITERATURY

Odborná literatura

[1] HANÁČEK Petr, STAUDEK Jan.: Bezpečnost informačních systémů (Metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií). Úřad pro státní informační systém 2000, s.297, ISSN 70-872-504-211

[2] HLAVICA J., LUKÁŠ, L., TKÁČIK T.: Řízení komunikační a informační podpory. Skripta, UO Brno, 2005, s. 155, ISBN 978-80-7318-799-6

[3] HŘEBÍČEK J, ŠTEFANÍK M.: Systémy integrovaného managementu, Masarykova universita 2008. [cit. 2010-05-16]. Dostupný z www: http:// www.fi.muni.cz

[4] IVANKA J.: Systemizace bezpečnostního průmyslu II, skripta FAI UTB, 2009

[5] JAŠEK, R. Informační a datová bezpečnost. Univerzita Tomáše Bati ve Zlíně. 2006. 140s. ISBN 80-7318-456-7.

[6] STAUDEK Jan.: Úvod do problematiky bezpečnosti IT, FI MU Brno, verze: podzim 2007. [cit. 2010-05-20] Dostupný z www: http://www.fi.muni.cz/usr/staudek/vyuka/

[7] STAUDEK Jan.: Budování bezpečnosti IT a analýza rizik, FI MU Brno, verze: podzim 2007. Dostupný z www: http://www.fi.muni.cz/usr/staudek/vyuka/

[8] STAUDEK Jan.: Standardizace bezpečnosti IT, FI MU Brno, verze: podzim 2007. Dostupný z www: http://www.fi.muni.cz/usr/staudek/vyuka/

[9] STAUDEK Jan.: Informační bezpečnost podle ISO / IEC 2700x, FI MU Brno, verze: podzim 2007. Dostupný z www: http://www.fi.muni.cz/usr/staudek/vyuka/

[10] STAUDEK Jan.: Kritéria hodnocení bezpečnosti IT, FI MU Brno, verze: podzim 2007. Dostupný z www: http://www.fi.muni.cz/usr/staudek/vyuka/

[11] KUNDEROVÁ Ludmila.: Informační bezpečnost, Ústav informatiky PEF MZLU v Brně, Dostupný z www: http://akela.mendelu.cz/~lidak

[12] ISO/IEC 27001, Informační technologie – Bezpečnostní techniky – Systémy menegementu bezpečnosti informací – Požadavky. [cit. 2010-05-10].

[13] EN ISO 9001:2000, Quality management systéme – Requirements (Systémy managementu jakosti – Požadavky)

[14] ISO/IEC 13335-1:2004, Information technology – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management (Informační technologie – Směrnice pro řízení bezpečnosti IT – Část 1: Pojetí a modely bezpečnosti IT.)

[15] ISO/IEC TR 13335-3:1998, Information technology – Guidelines for the Management of IT security – Part 3: Techniques for the management of IT security.
(Informační technologie – Směrnice pro řízení bezpečnosti IT – Část 3: techniky pro řízení bezpečnosti IT.)

[16] ISO/IEC TR 13335-4:2000, Information technology – Guidelines for the Management of IT security – Part 4: Selection of safeguards. (Informační technologie – Směrnice pro řízení bezpečnosti IT – Část 4: Výběr ochranných opatření.)

[17] ISO 19011:2002 Guidelines for duality and / or environmental management systéme auditing (Směrnice pro auditování systému managementu jakosti a / nebo systému environmentálního managementu)

[18] ISO/IEC Guide 73:2002, Risk management – Vocabulary – Guidelines for use standards

[19] CLC/TS 50398:2004. Poplachové systémy – Kombinované a integrované systémy - Všeobecné požadavky

Časopisy a katalogy

[20] SECURITY magazín, březen/duben 2010 [cit. 2010-05-30]

[21] Elektronické zabezpečovací systémy, Katalog 2008/2009, ADI – OLYMPO

[22] Průvodce strukturovanou kabeláží (od pracovního místa až po strukturovanou kabeláž) 2008/2009, legrand

[23] Elektronické systémy budov, Katalog produktů 2010-2011, Variant plus

Elektronické zdroje - Internet

[24] http://cs.wikipedia.org/wiki/Telekomunikace, [cit. 2010-05-09]

[25] http://www.adiglobal.cz/ , [cit. 2010-05-12]

[26] http://www.alcatel-lucent.com/wps/portal?COUNTRY_CODE=US&COOKIE_SET=false

[27] http://www.7marsyas.cz/reseni/bezpecnostni_systemy/access/, [cit. 2010-05-12]

[28] http://www.euroalarm.cz/

[29] http://www.ezu.cz/index.php?u=/certifikace-systemu-rizeni/isms-27001/&a=ArticleDisplay

[30] http://www.versasys.cz/isms-a-bezpecnost-informaci-138.html

[31] http://www.iso27000.cz/

[32] http://www.fi.muni.cz/usr/staudek/vystavelova/, [cit. 2010-05-16]

[33] https://akela.mendelu.cz/~lidak/bis/index.htm

[34] http://www.itil.cz/index.php?id=7

[35] http://www.ostravia.cz/files/ostravia_provozni_rad.pdf

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

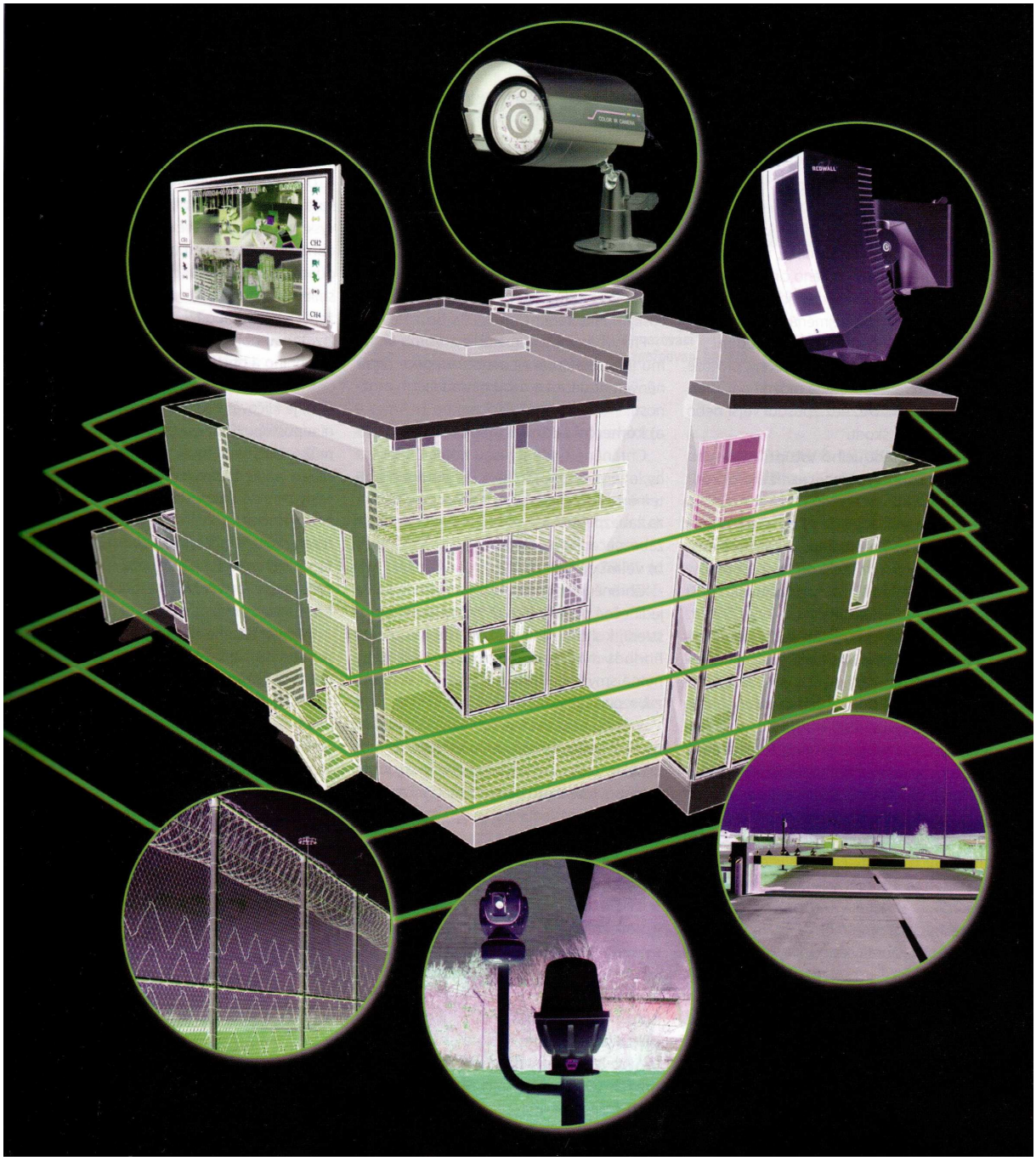
ACS	Access control systém (Systém kontroly přístupu)
BCP	Business continuity plan (Plán zachování kontinuity)
CAT6	Category 6 cable (Kategorie 6 kabel strukturované kabeláže)
CCD	Charge-Coupled Device (Snímací zařízení)
CCITT	Comité Consultatif International Télégraphique et Téléphonique (Mezinárodní poradní výbor pro telegraf a telefon)
CCTV	Close circuit television (Uzavřený televizní okruh)
DA	Diesel agregát
DDS	Domovní dorozumívací systémy
EKV	Elektronická kontrola vstupu
EPS	Elektrická požární signalizace
EZS	Elektrická zabezpečovací signalizace
FTP	File Transfer Protocol (Protokol aplikační vrstvy z rodiny TCP/IP)
GSM	Groupe Spécial Mobile (Globální Systém pro Mobilní komunikaci)
HD	Hard Disk (Pevný disk)
HDD	Hard Disk Drive (Pevný disk)
HW	Hardware (technické vybavení počítače)
I&HAS	Intruder and Hold-up Alarm Systems (Poplachové zabezpečovací a tísňové systémy)
ICT	Information and Communication Technology (Informační a komunikační technologie)
ID	Identifikace (Identifikátor)
IS	Information systém (Informační systém)
ISMS	Information Security Management Systém (Systém řízení bezpečnosti informací)
ISO	International Organization for Standardization (Mezinárodní organizace pro normalizaci)
IT	Information Technology (Informační technologie)
ITU	International Telecommunications Union (Mezinárodní telekomunikační unie)
LAN	Local Area Network
LCD	Liquid crystal display (Displej z tekutých krystalů)
MaR	Měření a regulace
MÚ	Mimořádná událost

MZS	Mechanické zabrané systémy
MW	Mikrovlnný
PC	Personal Computer (Osobní počítač)
PCO	Pult centrální ochrany
PČR	Policie České republiky
PDCA	Plan-do-check-act (Plánuj, udělej, zkontroluj, jednej)
PIN	Personal identification number (Osobní identifikační číslo)
PIR	Pasivní infračervený
PVC	Polyvinylchlorid
RJ12	Registred jack (Konektor – standardizované síťové rozhraní)
SHZ	Stabilní hasicí zařízení
SIM	Subscriber identity module (Účastnická identifikační karta)
SLA	Service Level Agreement (Dohoda o poskytované službě)
SMS	Short message service (Služba krátkých textových zpráv)
SOA	Statement of Applicability (Prohlášení o aplikovatelnosti)
SSL	Secure Sockets Layer (Vrstva bezpečných sonetů)
SW	Software (Programové vybavení)
UPS	Uninterruptible Power Supply (Nepřerušitelný zdroj energie)
VoIP	Voice over Internet Protocol (Technologie, umožňující přenos digitalizovaného hlasu v těle paketů rodiny protokolů UDP/TCP/IP)
VPN	Virtual Private Network (Prostředek pro propojení několika počítačů na různých místech internetu do jediné virtuální počítačové sítě)
VZT	Vzduchotechnika
ZOTK	Zařízení pro odvod tepla a kouře

SEZNAM OBRÁZKŮ

SEZNAM PŘÍLOH

PŘÍLOHA P I: PERIMETRICKÁ OCHRANA



Obr. 20 Příklad zabezpečení budovy, perimetrická ochrana [20]

PŘÍLOHA P II: INTELIGENTNÍ BUDOVA

Obr. 22 Příklad zabezpečení inteligentní budovy [23]

PŘÍLOHA P III: KAMEROVÝ SYSTÉM

Obr. 17 Příklad zabezpečení objektu pomocí kamerového systému [25]