Návrh nového zabezpečení budovy Policie ČR

The New Security Building Proposal for Police of the CR

Bc. Lukáš Staša

Diplomová práce
2013

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

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

Jméno a příjmení:	**Bc. Lukáš Staša**
Osobní číslo:	**A11357**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Návrh nového zabezpečení budovy Policie ČR**

Zásady pro vypracování:

1. **Popište současné technické řešení zabezpečení budovy policie.**
2. **Zpracujte současné organizační schéma provozu budovy a režimová opatření.**
3. **Analyzujte slabá místa v systému.**
4. **Zpracujte normy a předpisy vztahující se k tématu.**
5. **Navrhněte technické prostředky pro zabezpečení objektu.**
6. **Vyhodnoťte přínos navrhovaného řešení.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **ČESKO. Zákon č. 412 ze dne 21. září 2005 o ochraně utajovaných informací a o bezpečnostní způsobilosti jak vyplývá z pozdějších změn. In: Sbírka zákonů České republiky. 2012, s. 1890-1958. částka 47, ISSN 1211-1244.**
2. **ČESKO. Vyhláška č. 528 ze dne 14.12.2005 o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb. In: Sbírka zákonů České republiky. 2011, částka 155, s. 5888-5916. ISSN 1211-1244.**
3. **KINDL, Jiří. Projektování bezpečnostních systémů I. Vyd. 2. Zlín: Univerzita Tomáše Bati, 2007, 134 s. ISBN 978-80-7251-313-0.**
4. **KŘEČEK, Stanislav. Příručka zabezpečovací techniky. Vyd. 2. S.l.: Cricetus, 2003, 351 s. ISBN 80-902-9382-4.**
5. **LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management I. 1. vyd. Zlín: VeRBuM, 2011, 316 s. ISBN 978-80-87500-05-7.**
6. **LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management II. 1. vyd. Zlín: VeRBuM, 2012, 386 s. ISBN 978-80-87500-19-4.**
7. **MUSIL, Rudolf. Ochrana utajovaných skutečností. 1. vyd. Praha: Eurounion, 2001, 379 s. ISBN 80-858-5893-2.**

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

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

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

Ve Zlíně dne 8. února 2013

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práce se zabývá návrhem nového zabezpečení budovy Policie ČR. Teoretická část je věnována ochraně utajovaných informací, technickému zabezpečení budovy a integraci bezpečnostních systémů. V praktické části je provedena analýza současného stavu zabezpečení budovy s následným stanovením nových požadavků. V práci je proveden návrh nového technického zabezpečení tak, aby byly všechny bezpečnostní aplikace integrovány do kompaktního celku a to vše v kontextu ochrany utajovaných informací. Součástí je i návrh nového organizačního schématu budovy.

Klíčová slova: PZTS, detektor, CCTV, ACCESS, Integrace poplachových aplikací, návrh zabezpečení

ABSTRACT

The diploma thesis has been focused on the new design of Police Department building. The theoretical part has been devoted to the protection of classified information, technical security of the building and integrating security systems. In the practical part there has been analyzed the current state of security of the building, followed by the introduction of the new requirements. In that thesis there has been designed the new technical support so that all security applications were integrated into a compact. Everything should be according to the context of protection of classified information. It has also included the proposal for the new organizational scheme of the building.

Keywords: I & HAS, detector, CCTV, ACCESS, Integration of Alarm Application, the Security Design.

Nejdříve bych na tomto místě velmi rád poděkoval vedoucímu diplomové práce panu Ing. Rudolfovi Drgovi za trpělivost, inspiraci, podporu a jeho pomoc při vedení během tvorby této diplomové práce.

Poděkování patří také tvůrci řešení VAR-NET INTEGRAL, firmě VARIANT plus s.r.o., která mi poskytnula potřebné informace a konzultace.

Dále bych poděkoval své rodině a přítelkyni za jejich trpělivost a podporu během celého studia.

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 **9**
I. TEORETICKÁ ČÁST **11**
1. OCHRANA UTAJOVANÝCH INFORMACÍ **12**
1.1 UTAJOVANÁ INFORMACE 12
1.1.1 STUPNĚ UTAJENÍ 13
1.1.2 DRUHY ZAJIŠTĚNÍ OCHRANY UTAJOVANÝCH INFORMACÍ 14
1.2 FYZICKÁ BEZPEČNOST 15
1.2.1 PROJEKT FYZICKÉ BEZPEČNOSTI 16
1.2.2 ZABEZPEČENÉ OBLASTI A OBJEKTY 16
1.2.3 TECHNICKÉ PROSTŘEDKY OCHRANY UTAJOVANÝCH INFORMACÍ 17
1.2.4 HODNOCENÍ RIZIK 18
1.2.5 BODOVÉ HODNOCENÍ ZABEZPEČENÝCH OBLASTÍ A JEDNACÍCH OBLASTÍ 18
1.3 ROLE NÁRODNÍHO BEZPEČNOSTNÍHO ÚŘADU 19
1.3.1 CERTIFIKACE TECHNICKÝCH PROSTŘEDKŮ 20
2. TECHNICKÁ A MECHANICKÁ OCHRANA OBJEKTŮ **22**
2.1 POPLACHOVÉ ZABEZPEČOVACÍ A TÍSŇOVÉ SYSTÉMY 22
2.1.1 ÚSTŘEDNA PZTS 23
2.1.2 DETEKTORY MAGNETICKÉ 23
2.1.3 DETEKTORY PIR 24
2.1.4 DETEKTORY POHYBU ULTRAZVUKOVÉ A MIKROVLNNÉ 24
2.1.5 DALŠÍ DETEKTORY NARUŠENÍ 25
2.1.6 TÍSŇOVÉ HLÁSIČE 25
2.2 PŘÍSTUPOVÉ SYSTÉMY 25
2.2.1 PŘÍSTUPOVÝ BOD 26
2.2.2 PŘÍSTUPOVÁ PRÁVA A ZÓNY 27
2.3 UZAVŘENÝ TELEVIZNÍ OKRUH 27
2.3.1 LEGISLATIVNÍ POŽADAVKY Z HLEDISKA OCHRANY OSOBNÍCH ÚDAJŮ 28
2.3.2 IP KAMEROVÉ SYSTÉMY 28
2.3.3 SPECIÁLNÍ FUNKCE KAMEROVÝCH SYSTÉMŮ 29
2.4 MECHANICKÉ ZÁBRANNÉ SYSTÉMY 29
3. INTEGRACE POPLACHOVÝCH SYSTÉMŮ **31**
3.1 SYSTÉMOVÉ POŽADAVKY 31
3.2 SPECIFIKACE KONFIGURACÍ A STUPNĚ INTEGRACE 32
3.3 REZIDENČNÍ, KOMERČNÍ A MĚSTSKÉ SYSTÉMY 33
3.4 SYSTÉMOVÁ INTEGRACE A SYSTÉMOVÝ INTEGRÁTOR 34
3.5 HARDWAROVÁ INTEGRACE 35
3.6 SOFTWAROVÁ INTEGRACE 39
3.7 FUNKCE INTEGROVANÝCH SYSTÉMŮ 40
4. LEGISLATIVNÍ A TECHNICKÉ NORMY **42**

DÍLČÍ ZÁVĚR TEORETICKÉ ČÁSTI **43**
II. PRAKTICKÁ ČÁST **44**
5. ANALÝZA SOUČASNÉHO STAVU OCHRANY BUDOVY POLICIE **45**
5.1 STAVEBNĚ TECHNICKÝ POPIS ŘEŠENÉ BUDOVY 45
5.2 UMÍSTNĚNÍ STAVBY A ANALÝZA PERIMETRU 46
5.3 ANALÝZA PLÁŠŤOVÉ OCHRANY 47
5.4 ANALÝZA PROSTOROVÉ OCHRANY 47
5.5 ANALÝZA PŘEDMĚTOVÉ OCHRANY 49
5.6 ANALÝZA ORGANIZAČNÍHO SCHÉMATU 50
6. NÁVRH POŽADAVKŮ NA PROJEKT ZABEZPEČENÍ BUDOVY POLICIE **51**
6.1 POŽADAVKY NA PZTS 51
6.2 POŽADAVKY NA ELEKTRONICKOU KONTROLU VSTUPU 52
6.3 POŽADAVKY NA KAMEROVÉ SYSTÉMY 52
7. NÁVRH TECHNICKÉHO ZABEZPEČENÍ BUDOVY **54**
7.1 ZABEZPEČENÍ BUDOVY INTEGROVANÝM SYSTÉMEM NA BÁZI VAR-NET INTEGRAL 54
7.1.1 PZTS 55
7.1.2 PŘÍSTUPOVÝ SYSTÉM 62
7.1.3 KAMEROVÝ SYSTÉM CCTV 64
7.2 INTEGRAČNÍ HW 66
7.2.1 HARDWARE POTŘEBNÝ K REALIZACI INTEGRACE BEZPEČNOSTNÍCH APLIKACÍ 66
7.3 INTEGRAČNÍ SW 68
7.3.1 VAR-NET INTEGRAL 68
7.3.2 FUNKCE VAR-NET INTEGRAL NAD ÚSTŘEDNOU EVO 192 (PZTS + ACCESS) 69
7.3.3 JEDNOTLIVÉ MODULY SW VAR-NET INTEGRAL – LICENCE 69
7.4 ZABEZPEČENÍ ZABEZPEČENÝCH OBLASTÍ „V“ A „D“ 72
7.4.1 VYHODNOCENÍ HROZEB A STANOVENÍ MÍRY RIZIKA 72
7.4.2 NÁVRH PROSTŘEDKŮ PRO ZABEZPEČENÍ OBLASTÍ A BODOVÉ HODNOCENÍ POVINNÝCH A NEPOVINNÝCH PRVKŮ 74
7.4.3 VÝPOČET BODOVÝCH HODNOT 77
7.5 ORIENTAČNÍ CENOVÁ KALKULACE NAVRHOVANÉHO ŘEŠENÍ 79
8. NOVÉ ORGANIZAČNÍ SCHÉMA A BEZPEČNOSTNÍ DOPORUČENÍ **81**
DÍLČÍ ZÁVĚR PRAKTICKÉ ČÁSTI **86**
ZÁVĚR **87**
CONCLUSION **90**
SEZNAM POUŽITÉ LITERATURY **92**
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK **94**
SEZNAM OBRÁZKŮ **95**
SEZNAM TABULEK **97**
SEZNAM PŘÍLOH **98**

ÚVOD

Lidé si chrání svůj majetek a zdraví už odnepaměti. Dříve se využívalo k ochraně majetku zejména mechanických zábranných prostředků nebo se majetek vyšší hodnoty střežil přímo strážnou službou. V dnešní době se různé druhy ochrany běžně kombinují s elektronickými technickými prostředky.

S vývojem civilizace se změnil i význam chráněného zájmu. Prostá ochrana majetku a zdraví se rozšířila o ochranu informací. Informace mají mnohdy větší cenu než majetek, a proto je potřeba věnovat ochraně informací zvláštní pozornost. Na důraznou ochranu informací dbají v komerční oblasti především velké a nadnárodní firmy, které svůj úspěch a generování enormních zisků zakládají z velké části na strategických informacích a umění s těmito informacemi zacházet. Dalšími oblastmi, v nichž dochází k zásadní ochraně informací, je například armáda, policie, bezpečnostní informační služba apod. U těchto složek nedochází k ochraně informací za účelem generování zisků, ale především za ušlechtilým účelem ochrany vnější a vnitřní bezpečnosti státu. Jako bezpečnostní správce informačních systémů u Policie ČR, které jsou provozované v utajovaném režimu, si tuto skutečnost velmi dobře uvědomuji. Proto se v této práci zaměřím na ochranu budovy Policie ČR, kde je prioritou ochrany důkazní materiál, operativní informace u rozpracovaných případů a podobně.

Tato diplomová práce se bude zabývat návrhem ochrany budovy police a jejich chráněných zájmů. Řešená budova Police ČR je v současné době využívána po předešlých reorganizačních krocích pouze jako prostor pro policejní stanici. To se má ale změnit a budova má být využívána plnohodnotně. V budově se budou nacházet bezpečnostní složky jako je obvodní oddělení policie a služba kriminální police a vyšetřování. Touto změnou se výrazně změní význam chráněného zájmu, a proto je nutné navrhnout takové zabezpečení, které by odpovídalo požadavkům daných v platné legislativě a současným technickým standardům.

V současné době Policie ČR zabezpečuje své budovy s využitím poplachových zabezpečovacích a tísňových systémů, systémů pro kontrolu vstupu a kamerových systémů. Nicméně, tyto poplachové aplikace nejsou žádným způsobem integrovány v kompaktní celek a s ohledem na dnešní technickou vyspělost se stávající bezpečnostní systém jeví jako roztříštěný, nekompaktní a zastaralý. Proto se v této práci pokusím navrhnout, jak by takový integrovaný bezpečnostní systém mohl vypadat a pokusím

se také o vyčíslení orientačních nákladů na pořízení integrovaného technického zabezpečení. Součástí práce je také návrh prostředků pro ochranu utajovaných informací.

Teoretická část diplomové práce je zpracována a optimalizována tak, aby působila uceleně, kompaktně a zahrnovala ty nejdůležitější okruhy, které neodlučně souvisí s řešenou problematikou. Teoretická část je rozdělena do čtyř kapitol, kdy podstatná část teorie je obsažena v prvních třech kapitolách. První kapitola obeznamuje čtenáře s pojmem, významem a ochranou utajované informace a souvisejícími legislativními předpisy. Druhá kapitola se zabývá technickými a mechanickými prostředky, které se využívají na poli ochrany budov, majetku a informací. V další teoretické části je čtenář obeznámen s možnostmi a rozdělením integračních řešení s využitím v bezpečnostních aplikacích. V poslední části teorie jsou uvedeny normy, které se dotýkají daného bezpečnostního řešení a příbuzných oblastí.

Praktická část diplomové práce je soustředěna na samotné řešení daného problému. Tato část práce je rozdělena do čtyř kapitol. V první je provedena analýza současného stavu ochrany budovy police. Je zde také uvedený stavebně technický popis budovy a to, jak je situována. Dále je podroben analýze perimetr objektu, plášťová, prostorová a předmětová ochrana, včetně organizačního schématu budovy. V další kapitole je navrženo řešení možného zabezpečení budovy. Jsou zde kladeny požadavky na poplachový zabezpečovací a tísňový systém, kamerový systém, elektronickou kontrolu vstupu a to vše za předpokladu integrace těchto bezpečnostních aplikací. V předposlední kapitole diplomové práce je proveden návrh technických prostředků pro realizaci integrovaného řešení zabezpečení. Je zde navrhnut potřebný hardware a software tak, aby bylo vše v rámci bezpečnostního systému kompatibilní a funkční. V této části jsou také navrženy prostředky pro ochranu utajovaných informací tak, aby celkový bodový součet hodnot odpovídal legislativním požadavkům pro ochranu utajovaných informací. Součástí této kapitoly je i vyčíslení orientační ceny navrhovaného bezpečnostního řešení. V poslední části této diplomové práce je zpracován návrh nového organizačního schématu provozu budovy. Organizační schéma řeší provoz objektu, vstup a vjezd do areálu, režim pohybu návštěv nebo také například ostrahu a klíčové hospodářství.

Cílem práce je navrhnout integrovaný bezpečnostní systém a organizační opatření, která budou respektovat i základní principy ochrany utajovaných informací.

I. TEORETICKÁ ČÁST

1. OCHRANA UTAJOVANÝCH INFORMACÍ

Ochrana utajovaných informací je upravena zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále jen zákon ochraně utajovaných skutečností). Poslední novelizace zákona o ochraně utajovaných informací byla provedena zákonem č. 167/2012 Sb. Zákon č. 412/2005Sb. stanovuje, co je utajovaná informace, podmínky pro přístup k utajovaným informacím a další požadavky na jejich ochranu. K zákonu o ochraně utajovaných informací jsou vydány prováděcí předpisy – vyhlášky a nařízení vlády, které upřesňují obsah právní normy obsažené v tomto zákoně, konkrétně právní normy č. 522-529/2005 Sb. Jako příklad uvedu nařízení vlády č. 522/2005 Sb., kterým se stanoví seznamy utajovaných informací, dále vyhláška 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků nebo vyhláška č. 527/2005 Sb., o personální bezpečnosti, která se zabývá například stanovením vzorů v oblasti personální bezpečnosti a bezpečnostní způsobilosti fyzické osoby, kdy dále řeší postupy a způsoby žádosti o vydání osvědčení.

1.1 Utajovaná informace

Definice utajované informace je uvedena v §2 zákona O ochraně utajovaných informací jako:

„Informace v jakékoli podobě zaznamenaná na jakémkoliv nosiči označená v souladu s tímto zákonem, jejíž vyzrazení nebo zneužití může způsobit újmu zájmu České republiky nebo může být pro tento zájem nevýhodné.“ [1, §2]

Národní bezpečnostní úřad (dále NBÚ) zpracovává návrh seznamu utajovaných informací, kdy seznam utajovaných informací vydává vláda svým nařízením - nařízení vlády č. 522/2005 Sb.

Dle §2 z. č. 412/2005 Sb., vyzrazení utajované informace může způsobit újmu zájmu České Republiky. Zájmem České Republiky je zachování její ústavnosti, svrchovanosti, územní celistvosti, mezinárodních závazků, dále zajištění vnitřního pořádku, bezpečnosti, obrany a ochrana ekonomiky, života nebo zdraví fyzických osob.

Co se týče újmy, která může být způsobena České republice, tak dle §3 se újma člení na

- Mimořádně vážnou újmu
- Vážnou újmu

- Prostou újmu

Mimořádně vážná újma může mít za následek mimořádně velké ztráty na životech, bezprostřední ohrožení svrchovanosti, územní celistvosti, demokratických základů České republiky nebo rozsáhlé ohrožení zdraví obyvatel. Dále sem můžeme zařadit dlouhodobé poškození ekonomiky České Republiky nebo vážné poškození bojeschopnosti ozbrojených sil.

Vážná újma může způsobit ohrožení svrchovanosti, územní celistvosti, značnou škodu ve finanční, měnové nebo hospodářské oblasti, narušení vnitřního pořádku a bezpečnosti nebo ztráty na lidských životech nebo ohrožení zdraví obyvatelstva.

Prostá újma může mít za následek například ohrožení bezpečnosti jednotlivce, ohrožení bezpečnostních operací nebo činnosti zpravodajských služeb, zhoršení vztahů České republiky s cizí mocí. Dále sem lze zařadit zmaření nebo ztížení a ohrožení prověřování nebo vyšetřování zvlášť závažných zločinů.

Nevýhodné pro zájem České republiky dle §3 odst. 5 z. č. 412/2005 Sb., je například vyzrazení utajované informace, která bude mít za následek zmaření, ztížení nebo ohrožení prověřování a vyšetřování ostatních trestných činu, narušení důležitých nebo politických jednání, poškození významných ekonomických zájmů České republiky, ekonomických zájmů Evropské unie nebo jejího členského státu. [1] [4]

1.1.1 Stupně utajení

Utajovaná informace se na základě možné způsobené újmy nebo nevýhodnosti zájmům České Republiky rozděluje dle §4 z. č. 412/2005 Sb. do čtyř stupňů utajení:

*„a) **Přísně tajné**, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit mimořádně vážnou újmu zájmům České republiky,*

*b) **Tajné,** jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit vážnou újmu zájmům České republiky,*

*c) **Důvěrné**, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit prostou újmu zájmům České republiky,*

*d) **Vyhrazené**, jestliže její vyzrazení neoprávněné osobě nebo zneužití může být nevýhodné pro zájmy České republiky.“* [1, §4]

1.1.2 Druhy zajištění ochrany utajovaných informací

Zákon o ochraně utajovaných informací stanovuje v §5 druhy zajištění ochrany utajovaných informací. V následujících odstavcích jsou ocitovány jednotlivé druhy zajištění ochrany utajovaných informací (dále OUI) a následně jsou doplněny o některé informace, které jsem považoval za základní. Ochrana je tedy zajišťována:

„a) personální bezpečností, kterou tvoří výběr fyzických osob, které mají mít přístup k utajovaným informacím, ověřování podmínek pro jejich přístup k utajovaným informacím, jejich výchova a ochrana,“ [1, §5]

Personální bezpečnost je řešena §6-16 v II. hlavě zákona O ochraně utajovaných informací. Fyzické osobě se může umožnit přístup k utajovaným informacím, pokud jej nezbytně potřebuje k výkonu své funkce, pracovní nebo jiné činnosti, je držitelem oznámení o splnění podmínek k přístupu k utajovaným informacím stupně vyhrazené, je držitelem osvědčení fyzické osoby nebo dokladu a musí být poučená. Oznámení o přístupu k utajovaným informacím se vydává osobě, která je způsobilá k právním úkonům v plném rozsahu, dosáhla věku 18 let a je bezúhonná.

„b) průmyslovou bezpečností, kterou tvoří systém opatření k zjišťování a ověřování podmínek pro přístup podnikatele k utajovaným informacím a k zajištění nakládání s utajovanou informací u podnikatele v souladu s tímto zákonem,“ [1, §5]

Podnikateli, který nezbytně potřebuje k výkonu své činnosti přístup k utajovaným informacím, lze umožnit přístup, pokud doloží písemným prohlášením svou schopnost zabezpečit OUI (prohlášení podnikatele) nebo je držitelem osvědčení podnikatele dle §54 z. č. 412/2005 Sb.

„c) administrativní bezpečností, kterou tvoří systém opatření při tvorbě, příjmu, evidenci, zpracování, odesílání, přepravě, přenášení, ukládání, skartačním řízení, archivaci, případně jiném nakládání s utajovanými informacemi,“ [1, §5]

Pokud je informace charakterizována v seznamu utajovaných informací, je autor povinen vyznačit název, stupeň utajení, evidenční označení a datum vzniku, pokud není stanoveno jinak.

d) fyzickou bezpečností, kterou tvoří systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k utajovaným informacím, popřípadě přístup nebo pokus o něj zaznamenat, [1, §5]

Pro zajištění ochrany OUI v rámci fyzické ochrany se určují objekty, zabezpečené oblasti a jednací oblasti. Této problematice se věnuje vyhláška č. 528/2005 Sb., ve znění pozdějších předpisů. Fyzické bezpečnosti se budu věnovat podrobněji v kapitole 1.2 Fyzická bezpečnost.

„e) bezpečností informačních nebo komunikačních systémů, kterou tvoří systém opatření, jejichž cílem je zajistit důvěrnost, integritu a dostupnost utajovaných informací, s nimiž tyto systémy nakládají, a odpovědnost správy a uživatele za jejich činnost v informačním nebo komunikačním systému“ [1, §5]

Aby se mohla zpracovávat informace pomocí informačních systémů, musí být daný systém certifikovaný Národním bezpečnostním úřadem. Například ke zpracování utajovaných informací vyhrazených slouží informační systém (dále jen IS) VYDRA, informace stupně důvěrné se zpracovávají na IS DUDEK.

„f) kryptografickou ochranou, kterou tvoří systém opatření na ochranu utajovaných informací použitím kryptografických metod a kryptografických materiálů při zpracování, přenosu nebo ukládání utajovaných informací.“ [1, §5]

Kryptografické prostředky, které se užívají ke kryptografické ochraně utajovaných informací, musí být certifikovány Národním bezpečnostním úřadem. Kryptografický materiál je pak kryptografický prostředek, dokument a materiál k zajištění jeho funkce.

1.2 Fyzická bezpečnost

Aby nedošlo ke zneužití utajovaných informací, je důležitá funkce fyzické bezpečnosti, která tvoří jeden ze systému opatření OUI, které mají neoprávněné osobě zabránit nebo ztížit přístup k těmto informacím a popřípadě i zaznamenat pokus přístupu. V rámci fyzické bezpečnosti se určují objekty, zabezpečené oblasti a jednací oblasti.

- *„Objektem je budova nebo jiný ohraničený prostor, ve kterém se zpravidla nachází zabezpečená oblast nebo jednací oblast.*
- *Zabezpečenou oblastí je ohraničený prostor v objektu.*
- *Jednací oblastí je ohraničený prostor v objektu. Utajovanou informaci stupně utajení Přísně tajné nebo Tajné lze pravidelně projednávat pouze v jednací oblasti.“* [1, §24]

§24 odst. 5 z. č. 412/2005 Sb. hovoří o tom, že utajované informace mohou být zpracovávány v zabezpečené oblasti příslušné kategorie nebo vyšší nebo v objektu příslušné kategorie nebo vyšší v případě, že k utajené informaci nemá přístup neoprávněná osoba. V odůvodněných případech lze zpracovávat utajované informace i v objektu jiné kategorie (lze i mimo objekt), než je stupeň utajení informace, pouze s písemným souhlasem odpovědné osoby, popřípadě bezpečnostního ředitele.

Utajovaná informace se musí ukládat v zabezpečené oblasti příslušné kategorie, popřípadě vyšší. V zabezpečené oblasti může být uložena v trezoru, uzamykatelné skříni nebo jiné schránce za podmínek určených prováděcí vyhláškou 528/2005 Sb. [1]

1.2.1 Projekt fyzické bezpečnosti

Projekt fyzické bezpečnosti je dokument k objektu, ve kterém se nachází oblast podléhající některému stupni utajení. Pokud se v objektu nachází oblast kategorie přísně tajné, tajné a důvěrné dle §32 odst.1 z. č. 412/2005 Sb., potom tento dokument obsahuje: [1]

„a) určení objektu a zabezpečených oblastí, včetně jejich hranic a určení kategorií a tříd zabezpečených oblastí

b) vyhodnocení rizik

c) způsob použití opatření fyzické bezpečnosti

d) provozní řád objektu

e) plán zabezpečení objektu a zabezpečených oblastí v krizových situacích.“ [1, §32]

Pokud se v objektu nachází oblast kategorie vyhrazené dle §32 odst.2 z. č. 412/2005 Sb., potom musí obsahovat:

„a) určení objektu a zabezpečených oblastí, včetně jejich hranic a určení kategorií tříd zabezpečených oblastí a

b) způsob použití opatření fyzické bezpečnosti.“ [1, §32]

1.2.2 Zabezpečené oblasti a objekty

Zabezpečené oblasti a zabezpečené objekty, ve kterých probíhá zpracování nebo projednávání utajovaných informací, se zařazují do kategorií:

a) přísně tajné - PT
b) tajné - T

c) důvěrné - D
d) vyhrazené - V

Zabezpečené oblasti se pak dále zařazují do tříd dle přístupu k utajované informaci a to:

a) Třída I, kdy vstupem do dané oblasti dochází k seznámení s utajenou informací
b) Třída II, kdy vstupem do této oblasti nedochází k seznámení s utajenou informací

Vstup a výstup ze zabezpečené oblasti musí být kontrolován opatřením fyzické bezpečnosti, které jsou:

a) ostraha
b) režimová opatření
c) technické prostředky [1]

1.2.3 Technické prostředky ochrany utajovaných informací

Technické prostředky dle §30 z. č. 412/2005 Sb. jsou zejména:

„a) mechanické zábranné prostředky,

b) elektrická zámková zařízení a systémy pro kontrolu vstupů,

c) zařízení elektrické zabezpečovací signalizace,

d) speciální televizní systémy,

e) tísňové systémy,

f) zařízení elektrické požární signalizace,

g) zařízení sloužící k vyhledávání nebezpečných látek nebo předmětů,

h) zařízení fyzického ničení nosičů informací,

i) zařízení proti pasivnímu a aktivnímu odposlechu utajované informace.“ [1, §30]

Míra zabezpečení zabezpečených oblastí a jednacích oblastí se určuje pomocí bodových hodnot těchto opatření v závislosti na vyhodnocení rizik. Bodové hodnoty s nejnižší mírou zabezpečení jsou uvedeny ve vyhlášce 528/2005 Sb. Opatření fyzické bezpečnosti musí odpovídat alespoň nejnižší míře zabezpečení dané oblasti a stanoví se v závislosti na vyhodnocení rizik a stupni utajení informací. [1]

1.2.4 Hodnocení rizik

Hodnocení rizik je jedna z podmínek pro určení minimálního bodového ohodnocení dané zabezpečené nebo jednací oblasti a je jednou z nejdůležitějších oblastí bezpečnostní politiky organizace při OUI. Cílem je nejen popsat hrozbu, ale i stanovit riziko a zvážit rozsah možných následků. Hodnocení rizik je součástí projektu fyzické bezpečnosti. Hodnocení se provádí:

a) Identifikaci stupňů utajovaných informací a zjištěním jejich množství, které se v objektu vyskytují nebo budou vyskytovat, kdy se riziko posuzuje z toho hlediska, jaký by byl následek vyzrazení nebo zneužití utajovaných informací.
b) Popisem a vyhodnocením hrozeb, které mohou na utajované informace působit
c) Popisem a vyhodnocením zranitelnosti vůči hrozbám
d) Stanovením míry rizika: malé, střední, velké [2][3][4]

1.2.5 Bodové hodnocení zabezpečených oblastí a jednacích oblastí

Bodové hodnocení zabezpečených oblastí a jednacích oblastí vychází z přílohy č. 1, vyhlášky č. 528/2005 Sb. V příloze jsou obsaženy bodové požadavky ve formě „S“ nebo „SS“, které slouží k bodovým výpočtům a následnému porovnání, zda bodový součet dosahuje na potřebnou minimální hodnotu dané kategorie a odpovídá též bodům v závislosti na míře rizika. Každá kategorie má pro jednotlivé míry rizika povinné a nepovinné položky „S“. V tabulce č. 1 uvádím bodové hodnoty nejnižší míry zabezpečení pro oblast kategorie Přísně tajné. V tabulce č. 1 si můžeme povšimnout povinných položek S1 – úschovný objekt, S2 – zámek úschovného objektu, S3 – hranice objektu, S4 celkové hodnocení kontroly vstupu, S5 celkové hodnocení ostrahy. Zatímco S6 – celkové hodnocení ochrany perimetru není vyžadováno.

Tabulka 1: Bodové hodnoty nejnižší míry zabezpečení zabezpečené oblasti kategorie Přísně tajné [2]

ZABEZPEČENÁ OBLAST KATEGORIE Přísně Tajné	**Míra rizika**		
	malá	střední	velká
Povinné : (S1) + (S2) + (S3)	10	11	13
Povinné : (S4) + (S5) *	6	7	7
Nepovinné : (S6)	4	5	5
Celkový výsledek	**20**	**23**	**25**

Pro porovnání uvádím v tabulce č. 2, jaké bodové hodnoty postačí pro objekty kategorie Vyhrazené oproti kategorii přísně tajné uvedené v tabulce č. 1.

Tabulka 2: Bodové hodnoty nejnižší míry zabezpečení zabezpečené oblasti kategorie Vyhrazené [2]

ZABEZPEČENÁ OBLAST KATEGORIE Vyhrazené sloužící k ukládání utajované informace v komponentách informačního systému nebo kryptografickém prostředku nebo která vyžaduje zvláštní režim nakládání	
Povinné : (S1) + (S2) + (S3)	2
Nepovinné : (S4) + (S5) + (S6)	1
Celkový výsledek	**3**

Návrh technického zabezpečení zabezpečené oblasti tedy musí vycházet z bodových požadavků obsažených ve vyhlášce č. 528/2005 Sb. a v návaznosti musí být použity odpovídající certifikované zařízení. [2]

1.3 Role Národního bezpečnostního úřadu

Ústředním správním úřadem pro oblast ochrany utajovaných skutečností s celostátní působností je Národní bezpečnostní úřad (dále NBÚ) v Praze. Byl zřízen zákonem č. 148/1998 Sb. Stěžejním úkolem NBÚ v rámci utajovaných informací je zajišťování jednotného provádění ochrany. Dále vykonává funkci státního dozoru a metodickou činnost. Předmětem státního dozoru je kontrola dodržování metodických činností, které tedy zajišťují jednotné provádění ochrany. Dále NBÚ zajišťuje provádění bezpečnostních prověrek fyzických osob a organizací. K tomu patří i vydávání osvědčení příslušným subjektům. Úřad dále vykonává činnost související s mezinárodním stykem v oblasti utajovaných informací, vede registr utajovaných informací a plní závazky vyplývající z mezinárodních smluv. Dalším důležitým úkolem je certifikace technických, počítačových a kryptografických prostředků. Zajišťuje výzkum a vývoj a řídí kryptografickou ochranu utajovaných informací a zajišťuje kryptoanalytické služby. NBÚ dále vede evidenci případu neoprávněného nakládání s utajovanými informacemi. NBÚ tedy provádí a má tyto úkoly:

- bezpečnostní prověrky fyzických osob a organizací
- zabezpečuje ochranu utajovaných informací
- provádí certifikace technického prostředku, informačního systému, kryptografického prostředku, kryptografického pracoviště a stínící komory
- výzkum, vývoj a výrobu národních kryptografických prostředků

- vyvíjí a schvaluje národní šifrové algoritmy a vytváří národní politiku kryptografické ochrany
- je národním střediskem pro distribuci kryptografického materiálu
- je národním střediskem pro měření kompromitujícího elektromagnetického vyzařování
- ve stanovených případech povoluje poskytování utajovaných informací v mezinárodním styku
- je gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast [2] [7]

1.3.1 Certifikace technických prostředků

Dle §46 č. 412/2005 Sb. zajišťuje NBÚ certifikaci prostředků. Certifikace je postup, kdy NBÚ ověřuje způsobilost technických a jiných prostředků k tomu, aby mohly být využívány k ochraně utajovaných informací. Certifikáty jsou veřejnými listinami. V rámci certifikace systémů je zkoušení výrobků zajišťováno zkušební laboratoří. Tyto laboratoře musí splňovat všeobecné požadavky ČSN EN ISO/IEC 1725:2005. NBÚ vydává několik druhů certifikátů v závislosti na druhu a technice. Certifikáty jsou vydávány pro:

- Technické prostředky
- Informační systémy
- Kryptografické prostředky
- Kryptografické pracoviště
- Stínící komory

Certifikáty technického prostředku (obrázek č. 1) obsahují název a typ technického prostředku, zařazení prostředku do kategorie, evidenční číslo certifikátu, identifikaci držitele certifikátu, datum vydání a dobu platnosti, úřední razítko NBÚ. Výrobce, dovozce nebo distributor technického prostředku může žádat NBÚ o vydání certifikátu. Platnost certifikátu u technického prostředku stanoví NBÚ maximálně na dobu pěti let. Seznam certifikovaných technických prostředků s výjimkou prostředků certifikovaných na žádost uživatele technického prostředku, je zveřejňován na internetových stránkách NBÚ www.nbu.cz. NBÚ vydává certifikáty pouze na základě certifikátu shody (CE) vydaného akreditovaným orgánem pro následující technické prostředky:

- Mechanické zábranné prostředky

- Elektrická zámková zařízení a systémy pro kontrolu vstupu
- Zařízení elektrické zabezpečovací signalizace
- Tísňové systémy
- Zařízení fyzického ničení nosičů informací nebo dat [1] [2] [8]

Příloha č. 2 k vyhlášce č. 528/2005 Sb.

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD
Pošt. přihr. 49
150 06 Praha 56

Národní bezpečnostní úřad vydává podle § 46 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti

CERTIFIKÁT
technického prostředku

Evidenční číslo: ……..

……
(Název a typové označení technického prostředku)

Výrobce:
Sídlo/trvalý pobyt/ místo podnikání/adresa: IČ/ rodné číslo
Držitel:
Sídlo/trvalý pobytu/místo podnikání/adresa: IČ/ rodné číslo:

Tento certifikát potvrzuje ověření způsobilosti technického prostředku typu:

……

Bodové hodnocení technického prostředku podle přílohy č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků:

……

Platnost certifikátu do:
Datum vydání certifikátu:

Otisk úředního razítka

Podpis oprávněného zástupce

Přílohy:
(Příloha je nedílnou součástí certifikátu a lze je reprodukovat pouze společně)

Obrázek 1: Vzor certifikátu technického prostředku [2]

2. TECHNICKÁ A MECHANICKÁ OCHRANA OBJEKTŮ

Pokud budu vycházet z předešlé kapitoly, je nezbytně nutné k zabezpečení objektu technických a mechanických prvků ochrany. V následujících podkapitolách uvedu systémy pro ochranu objektů. Rozvoj elektroniky se v posledních desetiletích promítl i do elektronického zabezpečení objektů, kdy se využívají k detekci narušení různé fyzikální principy. V poslední době se již upouští od analogového zpracování informace a přechází se ke zpracování digitálnímu, které přináší řadu výhod.

V mnoha objektech se již využívá elektronická kontrola vstupu, kdy osoby můžeme zařadit např. do skupin a konkrétní skupině definovat přístupy do různých oddělení apod., kdy je možné tento systém využívat i jako docházkový s napojením do mzdových systémů.

Již řadu let se využívá ke kontrole objektu a dohledu, uzavřených kamerových systémů. Do nedávné doby byl signál zpracováván analogově, v současné digitální době by byla chyba vybavovat objekt analogovým systémem. Žádná ze z výše jmenovaných ochran by se neobešla bez mechanických zábranných systémů. Tyto systémy zabezpečují objekty od nepaměti, pouze dochází k jejich vývoji. Kombinací výše zmíněných systémů zabezpečení nám vzniká vícestupňová ochrana.

Následující podkapitoly jsou mimo jiné věnovány i základním detektorům, nejsou zde popsány všechny detektory narušení, ale pouze ty základní, u kterých předpokládám, že by mohly být využity k realizaci zabezpečení budovy Policie. Popisovat všechny ostatní detektory, by pak bylo v rámci této práce bezvýznamné a zbytečné.

2.1 Poplachové zabezpečovací a tísňové systémy

Jedná se o systém detektorů, tísňových hlásičů, ústředen, přenosových zařízení, záznamových zařízení, jejichž prostřednictvím je opticky nebo akusticky signalizováno narušení střeženého objektu (dle normy jen PZTS). Na manuální podnět reagují automatickou detekcí. Systémem PZTS se zabývá česká státní norma (dále jen ČSN) Poplachové systémy – Poplachové zabezpečovací a tísňové systémy - ČSN EN 50131. Všechny komponenty systému musí být navzájem kompatibilní a klasifikovány v souladu s jejich odolností vůči vlivům prostředí a dále musí být rozděleny do čtyř stupňů zabezpečení, kdy 1 je nejnižší a 4 nevyšší stupeň zabezpečení. Komponenty musí být voleny v souladu se stupněm zabezpečení a příslušnou třídou prostředí. Mezi základní

funkční požadavky PZTS patří detekce vniknutí, aktivace poplachu, detekce sabotáže a rozpoznání poruchy. Systém musí umožňovat zastřežení a odstřežení. [9]

2.1.1 Ústředna PZTS

Ústředna PZTS je centrálním zařízením zabezpečovacího a tísňového systému, který vyhodnocuje signály detektorů a v případě narušení objektu na základě signálu z detektoru vyhlašuje akustický nebo vizuální poplach. Poplach může ústředna předat na poplachové příjímací centrum (dále jen PPC) nebo na mobilní telefon například formou SMS. K ústředně mohou být také připojeny tísňové hlásiče. Ovládat ústřednu lze buď pomocí klávesnice, funkční klíčenky nebo pomocí počítače a speciálního software, pomocí webového prohlížeče nebo mobilního telefonu. Důležitou funkcí je také nastavení různých zón, které lze nezávisle na sobě zastřežit či odstřežit.

Ústředna se musí umísťovat do střeženého prostoru. Pokud je systém rozdělen do několika zón s různým stupněm zabezpečení, potom musí být ústředna umístěna v prostoru s nejvyšším stupněm zabezpečení. Ústředny často obsahují programovatelné výstupy (dále jen PGM), které lze naprogramovat tak, že na základě vyhodnocení signálu z detektoru lze ovládat jak poplachové, tak nepoplachové aplikace. PGM výstupy jsou realizovány pomocí tranzistoru nebo reléového prvku, kdy reléový výstup slouží ke spínání vyšších napětí a proudů. Lze také využít i spínače na DIN lištu v rozvodné skříni elektroinstalace domu a ovládat tak silové okruhy v objektu. Dle připojení smyček se ústředny dělí na analogové, sběrnicové, s bezdrátovou komunikací a ústředny hybridní. Ústředna může posílat signál na PPC například prostřednictvím připojením do jednotné telefonní sítě nebo bezdrátově GSM signálem. Stejným způsobem lze s ústřednou komunikovat, případně provádět i její konfiguraci. [4] [6]

2.1.2 Detektory magnetické

Jedná se o jedny z nejjednodušších detektorů. Jsou využívány především jako prvky plášťové ochrany pro střežení vstupních otvorů (oken a dveří) do budovy. Dále mohou být využívány k předmětové ochraně. Magnetické detektory jsou tvořeny jazýčkovými kontakty a permanentním magnetem. V případě, že se jazýčky nacházejí v magnetickém poli, jsou sepnuty. Pokud jsou z dosahu magnetického pole, dojde k jejich rozepnutí. Detektory obsahují i sabotážní kontakt, který detektor chrání před cizím magnetickým polem. [4]

2.1.3 Detektory PIR

Pasivní infračervený detektor (dále PIR) pracuje na elektromagnetickém principu. Využívá principu elektromagnetického záření, které vyzařuje každé těleso o teplotě vyšší než 0 K. PIR detektor tedy vyhodnocuje změnu vyzařování v infračerveném pásmu elektromagnetického vlnění. Z toho důvodu, že lidské tělo o teplotě 37st.C vyzařuje elektromagnetické vlnění o délce 9,3 μm, což je v pásmu infračerveného záření. Detekčním prvkem infračerveného záření je pyroelektrický snímač, který je schopen detekovat změnu záření, které na něj dopadá. PIR detektory patří k nejrozšířenějším detektorům, které jsou využívány k prostorové i perimetrické ochraně objektu. K hlavním výhodám patří nízká cena, nenáročnost výroby, nízká spotřeba energie. Nevýhodou je možnost rušení přímým slunečním zářením, osvětlením automobilů, mohou také reagovat na změnu teploty v místnosti, na činnost ventilace, pohyb žaluzií nebo závěsných předmětů. Detektory jsou opatřeny čočkami, které zajišťují lom paprsku tak, aby se soustředily na snímací prvek PIR. Vyrábějí se v klasické drátové nebo bezdrátové verzi. Nejvíce se využívají fresnelovy čočky. V současné době je nejmodernější fresnelova čočka se systémem LODIF pro detekci mrtvých zón. U PIR detektorů platí, že pokud nevidíme detektor, tak detektor nevidí ani nás a proto je nutné, aby detektory nebyly čímkoli stíněny. [4]

2.1.4 Detektory pohybu ultrazvukové a mikrovlnné

Ultrazvukové a mikrovlnné detektory pohybu se využívají pro perimetrickou i prostorovou ochranu střežených objektů. K detekci narušení zóny využívají změny kmitočtu vln. U ultrazvukových se kmitočty pohybují v rozmezí 20-60 kHz a mikrovlnné detektory pracují v pásmu 1-10 GHz. Činnost těchto detektorů je založena na aplikaci Dopplerovu principu, který využívá zpětného odrazu vyslané vlny. Detektor tedy musí mít vysílač a přijímač. Takovéto zařízení pak nazýváme jako aktivní detektor.

Pro dobrou detekci narušitele musí být detektor umístěn tak, aby se narušitel pohyboval ve směru k detektoru nebo od něj. Pokud by se pohyboval v konstantní vzdálenosti, nemuselo by dojít ke spolehlivé detekci. V jednom prostoru může být užito i více detektorů, ale pouze za podmínky, že budou pracovat na různých frekvencích, aby se vzájemně neovlivňovaly a nevyvolávaly falešný poplach. Ultrazvukové detektory by se neměly instalovat nad topná tělesa, nad závěsy a neměly by se užívat v místnosti, ve kterých se mohou vyskytovat široké spektra zvuku, například by neměly být umístěny v blízkosti

telefonů apod. U mikrovlnných detektorů vlny procházejí sklem a k vyvolání poplachu může dojít i narušením mimo zónu. Vlny také mohou procházet tenkými stěnami. Vyrábějí se v drátovém i bezdrátovém provedení. V problematických prostředích se využívají kombinované detektory ultrazvuk-PIR nebo mikrovlna-PIR. [4] [10]

2.1.5 Další detektory narušení

Detektorů narušení je celá řada. Výše popsané jsou jen jedny ze základních nejpoužívanějších, jak jsem již avizoval v úvodu druhé kapitoly. Např. k perimetrické ochraně mohou být využity mikrovlnné bariéry, štěrbinové kabely nebo zemní tlakové hadice. U plášťové ochrany se vyžívají také poplachové fólie, vibrační detektory. K předmětové ochraně se mohou využívat tlakové detektory, závěsová nebo kapacitní. [4]

2.1.6 Tísňové hlásiče

Tísňové hlásiče slouží uživateli k manuálnímu úmyslnému vyvolání poplachového stavu. Je několik typů tísňových hlásičů a to veřejné, osobní a skryté. Veřejné hlásiče slouží veřejnosti k vyvolání poplachu v případě nebezpečí. Osobní hlásič slouží konkrétní osobě a je ve formě bezdrátové klíčenky. Skryté tísňové hlásiče jsou využívány například u bank nebo jiných objektů, kde dochází k napadení a je potřeba skrytě vyvolat tíseň. [6] [11]

2.2 Přístupové systémy

Je nutné rozlišit přístupový a docházkový systém. Docházkový systém slouží pouze k identifikaci osoby a evidenci pracovní doby. Tento systém je pak integrován do mzdových aplikací. Přístupové systémy tvoří část bezpečnostní politiky ve firmách. Úkolem přístupového systému je řízený přístup do různých oblastí budovy a s tím je i spojená evidence průchodů konkrétní osoby. Norma upravující provoz je ČSN 50 133.

Přístupový systém se skládá z hardwarové a softwarové části. Hardwarovou část tvoří snímač pro identifikaci (čtečka, klávesnice apod.), identifikační prvky, převodník, napájecí a záložní zdroj, elektrický dveřní zámek, případně turniket, závora a podobně. Software vyhodnocuje identifikační údaje a rozhoduje, zda osobě umožnit přístup nebo přístup zamítnout.

Přístupové systémy můžeme rozdělit na:

a) Autonomní

   Pracují bez obslužného softwaru nezávisle na počítači. Všechna přístupová práva jsou uložena v jednotce kontroleru. Paměť obvykle umožňuje definovat řádově desítky uživatelů. Jedná se o nejjednodušší přístupový bod. Nevíce se využívá u samostatných prostupů s menší četností pohybu osob.

b) Modulární systémy

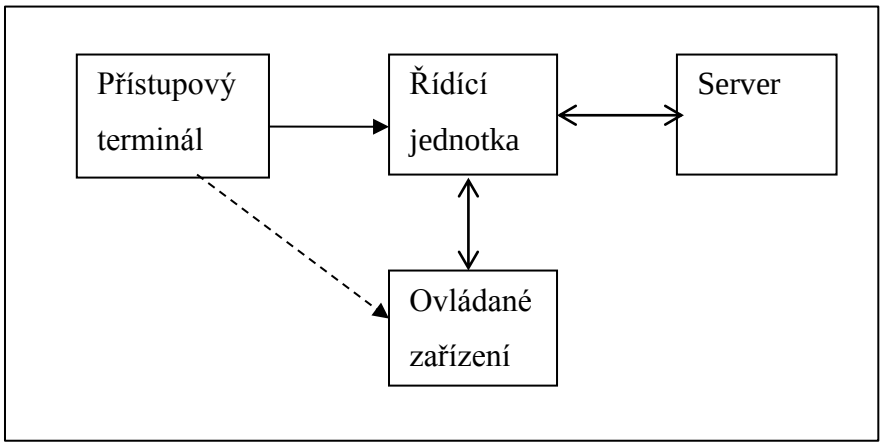
   Jedná se o rozsáhlejší systémy. Jsou tvořeny větším množstvím přístupových bodů, řídícími jednotkami a serverem. Nejčastěji se využívá sběrnicová nebo hvězdicová topologie, kdy je ústředna jako centrální prvek a zajišťuje samotné ověření přístupových práv, časových filtrů a podobně.

Přístupový systém lze také integrovat s jinými systémy, např. u stravovacího systému lze využívat stejné identifikační médium. Integrovat lze také se systémem poplachového zabezpečovacího a tísňového systému, kdy prostřednictvím identifikace osoby může být odstřežena konkrétní zóna a při odchodu – „odhlášení se z místnosti“ dojde k automatickému zastřežení, pokud ovšem v daném objektu není další osoba.

Přístupový systém nahrazuje manipulaci s velkým množství klíčů. Identifikace osoby probíhá například pomocí čipu integrovaného do klíčenky, PINu, přístupové karty nebo biometrických prvků. Identifikace se může zesílit i tím, že dojde k identifikaci osoby pomocí čipu a zadáním osobního kódu. V současné době se začíná rozšiřovat biometrická identifikace osob. Biometrická identifikace vychází z toho, že některé anatomické a behaviorální charakteristiky, jsou pro danou osobu individuální. Identifikace může pak probíhat analýzou otisku prstu, oční sítnice a duhovky, tvaru krevního řečiště apod. [4]

2.2.1 Přístupový bod

Přístupový bod je základním prvkem celého přístupového systému. Základní jednoduché blokové schéma je uvedeno na obrázku č. 2. Skládá se ze zařízení pro identifikaci osoby. To je například čtečka čipových karet nebo čtečka otisku prstů atd. Identifikační údaje jsou pak předány do řídící jednotky, která rozhodne, zda má osoba přístup nebo ne. Pokud má osoba umožněný přístup, řídící jednotka vyšle signál pro odemčení například elektronického zámku nebo turniketu. Server slouží k evidenci přístupových údajů, konfiguraci řídící jednotky a podobně. [4]



Obrázek 2: Blokové schéma přístupového bodu.

2.2.2 Přístupová práva a zóny

Systém umožňuje nastavit každému uživateli přístupová práva do objektů. Je ale také možné vytvářet přístupové profily a tyto aplikovat na zaměstnance. Například profil ekonomické oddělení bude přiřazen pouze pracovníkům, kteří na daném oddělení pracují a do jiných oddělení jim bude přístup zamítnut Přístupový systém také umožnuje sledovat pohyb a přítomnost osob v jednotlivých zónách. Je možné nastavit i časové omezení, kdy budou rozdílné přístupy v noci, o svátcích nebo víkendech. [4]

2.3 Uzavřený televizní okruh

Jedná se o systém, který slouží k dálkové vizuální kontrole objektů a osob. Je to systém tvořený sadou kamer, zobrazovacím zařízením, záznamovým zařízením, systémem přenosu video signálu a ovládacími zařízeními kamer. Často se označuje zkratkou CCTV Closed circuit television – uzavřený televizní okruh. Tuto problematikou se zabývá norma ČSN EN 50 132 Poplachové systémy – CCTV sledovací systémy pro použití v bezpečnostních aplikacích. Kamerové systémy se dělí na analogové, digitální a hybridní. V současné době jsou analogové systémy na ústupu a standardem se stává kompletní digitalizace celého systému, v kterém se využívají digitální IP kamery, digitální přenos dat a digitální záznamové zařízení. Proto v této práci nebudu věnovat pozornost analogovým systémům a zaměřím se pouze na digitální IP systémy.

2.3.1 Legislativní požadavky z hlediska ochrany osobních údajů

Dle §16 z. č.101/2000Sb., kdo hodlá zpracovávat osobní údaje je povinen tuto skutečnost písemně oznámit Úřadu pro ochranu osobních údajů. Oznámení musí obsahovat například účel zpracování, identifikační údaje správce, zdroje osobních údajů, popis způsobu zpracování osobních údajů apod. Úřad pro ochranu osobních údajů vydal v roce 2006 stanovisko, kdy provozování kamerového systému je považováno za zpracování osobních údajů v případě, že je prováděn záznam obrazových nebo zvukových záběru za účelem jeho možného využití k identifikaci fyzických osob. Provozovatel – správce je pak povinen tuto skutečnost oznámit písemně Úřadu pro ochranu osobních údajů. Výjimka v oznamování je stanovena §18 z. č.101/2000Sb., například pro Policii ČR nebo Vězeňskou službu. Systém, který nepodléhá ochraně osobních údajů a nemusí být registrován, je takový, kde dochází pouze k monitoringu scény bez pořizování záznamu nebo pokud je záznam pořizován v nízkém rozlišení, které neumožňuje identifikaci osoby. Rovněž systém nepodléhá registraci, pokud se monitorují velké haly apod., kdy opět nesmí být osoba identifikovatelná na kamerovém záznamu. [12] [13]

2.3.2 IP kamerové systémy

IP kamery jsou na trhu přibližně 10 let, za tu dobu prošly velkým vývojem, který se do současnosti nezastavil. IP kamerové systémy mohou být jak v uzavřeném okruhu, tak v otevřeném okruhu. Důležitým prvkem celého systému je IP kamera, ta je tvořena objektivem, obrazovým snímačem CCD nebo CMOS, procesory pro digitalizaci signálu a rozhraním pro připojení do sítě. Hlavním rysem je, že kamera má svoji IP adresu, takže můžeme ke kameře přistupovat z jakéhokoli počítače v síti s využitím webového prohlížeče. Kamera je vlastně dalším prvkem firemní datové sítě LAN. Kamera může disponovat konektory pro koaxiální kabel, RJ45 pro zapojení do LAN nebo může signál předávat bezdrátově technologií WiFi. Veškeré digitální zpracování obrazu je prováděno v samotné kameře. Po zpracování obrazu je digitální signál již v komprimovaném stavu odesílán na komunikační rozhraní. Využitím komprese je ušetřena i část přenosového pásma a nedochází k zahlcení datové sítě.

Kamery jsou konstruovány pro venkovní nebo interní užití a vyrábějí se také v provedení antivandal, které je odolné mechanickému poškození. Kamery mohou být fixní nebo PTZ. U fixních kamer je při instalaci pevně nastavena snímaná scéna. PTZ kamery obsahují polohovací mechanizmy, kdy s kamerou můžeme měnit ohniskovou vzdálenost, její

vertikální a horizontální natočení, umožňující monitoring rozsáhlého prostoru. K těmto kamerám patří například kamery typu dome, které se ovládají pomoci joysticku. K záznamu signálu z IP kamer se pak využívá IPkordéru, kdy celková doba záznamu je omezena velikostí pevných disků, ale také záleží na tom, v jaké kvalitě bude obraz uchováván. Pro rozsáhlé systémy se využívají k záznamu disková pole s kapacitou řádově v TB. [4] [5]

2.3.3 Speciální funkce kamerových systémů

Mezi speciální funkce kamerových systémů patří PTZ autotracking. Jedná se o systém, který je schopen detekovat narušení a cíl dále sledovat v jeho pohybu pomocí pohybových funkcí kamery. Je možno využívat funkce multi-autotracking, kdy si kamery mezi sebou předávají sledovaný objekt. V tomto případě musí pak všechny kamery funkci autotrackingu podporovat.

Ke speciálním funkcím také patří počítání osob. Osoby se počítají na základě analýzy obrazu. Systémy mohou být také využity k perimetrické ochraně, kde si navolíme střežené zóny a pokud se v zóně objeví narušitel, dojde k vyhlášení poplachu. Systémy se využívají také k detekci zanechaného předmětu, kdy slouží především k detekci nástražných výbušných systémů apod. [5]

V současné době se stále více využívá kamerových systému pro sledování a evidenci průjezdů vozidel. Kamera snímá obraz s projíždějícím vozidlem a software převádí řetězec v RZ vozidla do textové podoby a ukládá ho s časem průjezdu a fotografií do databáze. Toto se pak využívá pro dohledávání zájmových vozidel, které byly například využity k páchání trestné činnosti.

Řada současných kamer na trhu je vybavena i poplachovými vstupy a výstupy umožňující například automaticky zacílit na scénu PTZ kamerou do místa, kde došlo k detekci narušení. Při narušení může být obrázek odeslán na email nebo zájmová videosekvence uložená do záznamového zařízení. Využití těchto vstupů je opravdu široké.

2.4 Mechanické zábranné systémy

Mechanické zábranné systémy neodmyslitelně patří k základní ochraně objektů a předmětů. Tyto systémy zabezpečují objekty a předměty od nepaměti, pouze dochází k jejich vývoji a integraci s jinými zabezpečovacími systémy. Mezi mechanické zábranné systémy patří všechny mechanické prvky, které stěžují násilné vniknutí osoby do

chráněných objektů. Smyslem mechanických zábranných systémů je také to, aby jejich možné překonání trvalo co nejdelší dobu. Bez mechanické ochrany objektu také nebude žádná pojišťovna plnit své závazky v oblasti pojištění proti krádeži vloupáním. Mechanickými zábrannými systémy se zabývají normy ČSN P ENV 1627-1630, ČSN 1303,1906,12320, 1143-1,916010 a norma ČSN 165110.

Pokud se jedná o obvodovou ochranu, tak sem patří například ploty, zdi, podhrabové zábrany, ostnaté dráty a podobně. Do plášťové ochrany můžeme zařadit okna, dveře, mříže. Mezi prvky předmětové ochrany řadíme trezory, přenosné pokladny nebo speciální zavazadla pro přepravu cenin. Úschovné objekty, které jsou užívány k ukládání utajovaných informací, musí být certifikovány NBÚ. [11]

3. INTEGRACE POPLACHOVÝCH SYSTÉMŮ

S rozvojem techniky a elektroniky rostou i požadavky zákazníků, kteří chtějí technické a elektronické možnosti zabezpečení využívat. Pokud se v současné době projektuje bezpečnostní systém, je kladen také důraz na jeho maximální integraci s ostatními poplachovými a nepoplachovými aplikacemi, samozřejmě s ohledem na finanční možnosti zákazníka. Integrace je cesta ke zvyšování účinnosti stávajících systémů s možností efektivního řízení krizových situací a optimalizací ekonomických nákladů vynaložených na energie. Můžeme také získat předpoplachové informace o zvláštním chování osob v daném objektu, popřípadě v jeho blízkosti. Je možné získat kontrolu o pohybu osob v budově pomocí přístupových systémů s návazností na mzdový systém. Norma, která se zabývá problematikou těchto integrací je norma ČSN CLC/TS 50 398 Poplachové systémy - Kombinované a integrované systémy.

Integrovaný poplachový systém je definovaný jako systém mající jedno nebo více společných zařízení, alespoň jedním z nichž je poplachová aplikace. Systém je tedy tvořen poplachovými a nepoplachovými aplikacemi.

- **Poplachová aplikace** je určena na ochranu života, majetku nebo prostředí, patří sem: PZTS, systémy přivolání pomoci, poplachový systém výtahů, poplachový systém vlivu prostředí, CCTV, ACS, EPS.
- **Nepoplachová aplikace** je systém určený k ovládání a jehož primární funkcí není ochrana života nebo majetku. Patří sem: řízení osvětlení v budově, ventilace, řízení energetických systémů atd. [6] [14]

3.1 Systémové požadavky

Při návrhu integrovaných poplachových systémů je nutné vyloučit možnost vzájemného ovlivnění všech aplikací a musí být možnost přenosu povelových signálů mezi aplikacemi. V návrhu se musí definovat provozní podmínky celého integrovaného systému. V systému musí být normou definovány přístupové úrovně bez možnosti neoprávněného přístupu jiným aplikacím. Musí existovat možnost detekce poruchy na společném zařízení a tato porucha musí být indikována ve všech dotčených aplikacích. Druhů signalizace informací je celkem šest a s různou prioritou. Níže uvádím druhy signalizace seřazené dle priority.

1. poplachové signály (ochrana života, požár, napadení)
2. poplachové signály (ochrana majetku, vniknutí do objektu)

3. poplachové signály ostatní
4. poruchové signály (ochrana života a majetku)
5. poruchové signály ostatní
6. informace z nepoplachových signálů

Je důležité, aby jakákoli činnost aplikace nezamezila indikaci poplachu. Musí být signalizován stav, kdy existují poplachy z více než jedné aplikace. Při vzájemném propojení zařízení, které splňují a které nesplňují aplikační normy, je nutné, aby systém akceptoval pouze povely aplikačních norem, neidentifikovatelné signály nesmí mít negativní vliv na systém. Je také důležité dodržení toho, aby všechna zařízení byla monitorovatelná a signalizovala sabotáž. Pokud jde o zpracování signálů v doplňkovém zařízení, nesmí být překročeno 150% doby specifikované v aplikační normě. Před předáním systému zákazníkovi musí být ověřena provozuschopnost každé aplikace v normálním provozním stavu a v předpokládaném poruchovém stavu. [6] [14]

3.2 Specifikace konfigurací a stupně integrace

V Normě ČSN CLC/TS 50 398 jsou uvedeny 3 konfigurační typy integrovaných poplachových signálů.

- **typ 1** – Kombinace a integrace jednoúčelových poplachových systémů a jednoúčelových nepoplachových systémů.
- **typ 2A** – Kombinace a integrace poplachových systémů a nepoplachových systémů, které používají společné přenosové trasy a společná zařízení. Porucha v jakékoli aplikaci nemá žádný negativní vliv na jakoukoli další poplachovou aplikaci, čehož se dosahuje redundancí neboli nadbytečností.
- **typ 2B** - Kombinace a integrace poplachových systémů a nepoplachových systémů, které používají společné přenosové trasy a společná zařízení. Porucha v jedné aplikaci může mít negativní účinek na jinou aplikaci v systému.

Existují tří různé stupně integrace, které charakterizují úroveň kompletnosti a míru homogenizace systému.

Integrační stupeň 1

Jedná se o základní stupeň integrace, která je provedena v rámci jednoho bezpečnostního systému. Příkladem může být systém kontroly vstupu, v kterém jsou čtečky karet,

klávesnice, monitorovací prvky, systém výdeje karet a správy uživatelských dat integrovány do jednoho systému.

Integrační stupeň 2

Jde o vyšší stupeň integrace v rámci několika bezpečnostních systémů. Příkladem může být integrace systému kontroly vstupu se zabezpečovací signalizací a kamerovým systémem do společného uživatelského rozhraní. Je zde vazba mezi systémy.

Integrační stupeň 3

Představuje nejvyšší stupeň integrace bezpečnostních a IT technologií. Například integrace systému kontroly vstupu s vnitřní komunikací s dalšími aplikacemi jako je mzdový systém pro výpočet mzdy dle odpracovaných hodin. [6] [14]

3.3 Rezidenční, komerční a městské systémy

Integrované bezpečnostní systémy můžeme rozdělit dle toho, v jaké oblasti jsou využívány. Rozdělujeme je na komerční, rezidenční a městské systémy. Všechny tyto integrované systémy se liší:

- Technologií aplikací a integračních prvků
- Způsobem ovládání
- Prioritou nasazení
- Požadavky uživatele

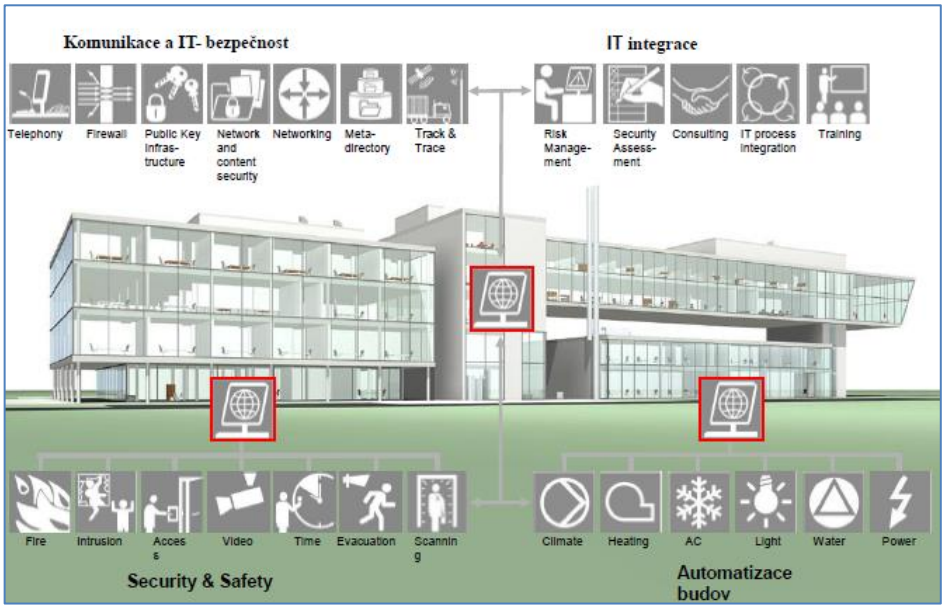
Ke kritériím výběru integrovaného systému patří: bezpečnostní hledisko, funkce a vazby, ekonomická náročnost, legislativní požadavky, individuální požadavky uživatele. Co se týká negativních dopadů nasazení integrovaných systémů, tak těch je několik. Patří sem: negativní mezi systémové interakce, redundance funkcí, snížení transparentnosti systému, vyšší nároky na obsluhu (znalost manuálů) a servis.

Rezidenční systémy

U rezidenčních systémů by se dalo říci, že hlavním požadavkem na integraci systémů je jejich provázanost a ovládání technologií z různých míst. To vše hlavně kvůli komfortnímu bydlení. Integrovaný systém pak řídí inteligentní osvětlení domu, vytápění, klimatizaci, zavlažování, rolety atd. Další prioritou nasazení je pak zvýšení bezpečnosti objektu. Pozitivní je také to, že díky řízení teploty v objektu dochází i ke snížení energetických nákladů objektu.

Komerční systémy

U komerčních integrovaných systémů (obrázek č. 3) dochází ke zvýšení efektivity a zjednodušení správy rozsáhlých budov a objektů. Důvodem nasazení je zvýšení úrovně zabezpečení. Zvyšuje přehled o situaci v objektu a lze lépe řešit krizové stavy. K ekonomickým přínosům patří snížení nákladů na energie (vytápění, elektřina, voda). K výhodám také patří snížení nákladů na zabezpečení ochrany objektu – není potřeba tolika strážných. Tento model využívají vodohospodářské subjekty, orgány státní správy, finanční instituce nebo telekomunikační společnosti.



Obrázek 3: Možnosti aplikace integrovaných systémů v komerčních objektech [6]

Městské systémy

Městské integrované systémy se využívají především z bezpečnostních důvodů. Slouží ke zvýšení bezpečnosti občanů v rámci primárních preventivních opatření kriminality. Hlavní součástí těchto systémů je městský kamerový systém, dále mohou být systémy integrovány s varovnými systémy – zobrazení stavu sirén a jejich ovládání atd. [6]

3.4 Systémová integrace a systémový integrátor

Systémovou integrací se rozumí spojení heterogenních subsystémů v jeden funkční celek. K integraci vedou požadavky zákazníků a snaha o zjednodušení automatizačních procesů. Systémová integrace by neměla být chápána jako produkt, ale měla by být chápána

především jako dodávka služeb. Systémová integrace umožňuje systémovou kontrolu: kontrola nad instalovanými technologiemi, minimalizace chyb způsobených obsluhou, možnost aplikace řízení typu „co se má stát když“. Integrovaný systém je navržen jako celek z různých komponentů a to i od různých výrobců a je dodáván jako celek služeb.

Formy integrace

- **Technologická integrace** – integrace PZTS, CCTV, ACS, řízení vytápění, zavlažování atd.
- **Funkční integrace** – sledování odpracované doby na zakázkách, přehled o stavu zakázek, přehledy o odstávkách stroje…
- **Integrace uživatelského rozhraní –** centrální ovládání poplachových a nepoplachových aplikací pomocí ovládacích panelů, PC nebo mobilního telefonu
- **Datová integrace** – na serveru jsou integrovány data z docházkových systémů, které jsou využívány například pro mzdové informační systémy
- **Metodická integrace** – zabezpečuje metodiku při registraci návštěv a stanovuje pravidla pro jejich doprovod, blokace vstupu nežádoucím osobám atd.

Systémový integrátor

Jak již bylo řečeno, integrovaný systém je dodáván především jako služba a ne jako produkt. Je dodáván jako celek služeb, které zahrnují: konzultace, bezpečnostní posouzení, projektování, implementace, instalace, školení a servis. Systémový integrátor je tedy firma, která zajišťuje komplexní realizaci systémové integrace. Pracovníci systémového integrátora musí mít rozsáhlé znalosti a schopnosti v oblasti poplachových a nepoplachových systémů, silnoproudých a slaboproudých systémů, nevýrobní automatizace. Navrhují architekturu aplikací a provádějí hardwarové konfigurace. Systémový integrátor by měl být vybírán dle toho, jak dlouho působí na trhu, jak je finančně stabilní, dle referencí, dle délky poskytované záruky. Samozřejmostí by také mělo být, aby systémový integrátor vlastnil potřebné certifikáty pro svoji činnost. [6]

3.5 Hardwarová integrace

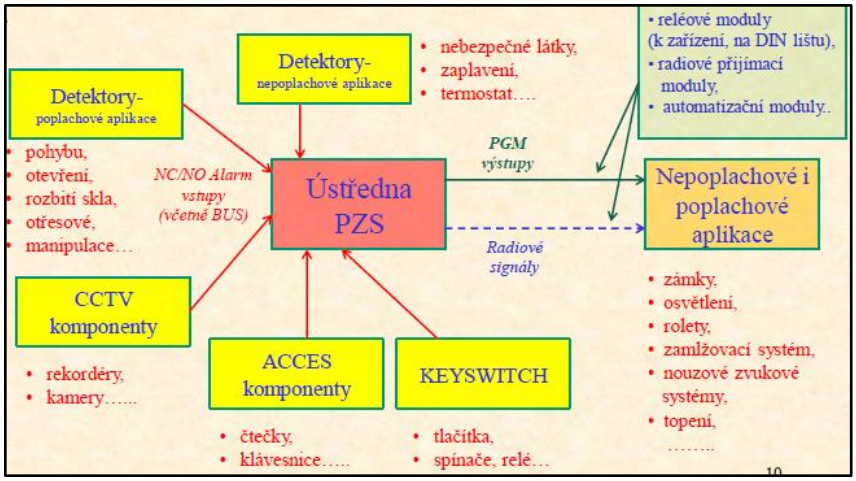
Aby všechny aplikace mezi sebou komunikovaly, je potřeba hardwarové a softwarové integrace. Hardwarová integrace řeší vzájemné propojení vstupů a výstupů různorodých systémů v jeden celek. K hardwarovým způsobům integrace lze zařadit i automatizační

systémy, které nabízí ovládání různých technologií v budově, kdy lze k tomuto systému připojit i zabezpečovací prvky. Mezi modely hardwarové integrace patří:

- Integrace IN/OUT
- PZTS jako integrační prvek – modulární systémy
- Automatizační systém jako integrační prvek

Integrace IN/OUT

Jedná se o vzájemné propojení systémů prostřednictvím jejich vstupů a výstupů (obecné schéma na obrázek č. 4). Tento typ integrace se často využívá a jde o nejstabilnější variantu integrace systémů. U rozsáhlejších aplikací může být tato integrace technologicky náročná, protože je velká náročnost na počty vstupů a výstupů. Integrace IN/OUT je vhodná k přenosu stavových informací jednotlivých systémů. Velkou výhodou je, že se systémy vzájemně negativně neovlivňují, kdy porucha jedné aplikace nemá negativní vliv na ostatní. Ke kladům patří také to, že v systému lze použít komponenty bez ohledu na výrobce a komunikační protokoly. Může být použito zařízení, které dokáže přepínat mezi otevřeným a uzavřeným okruhem.

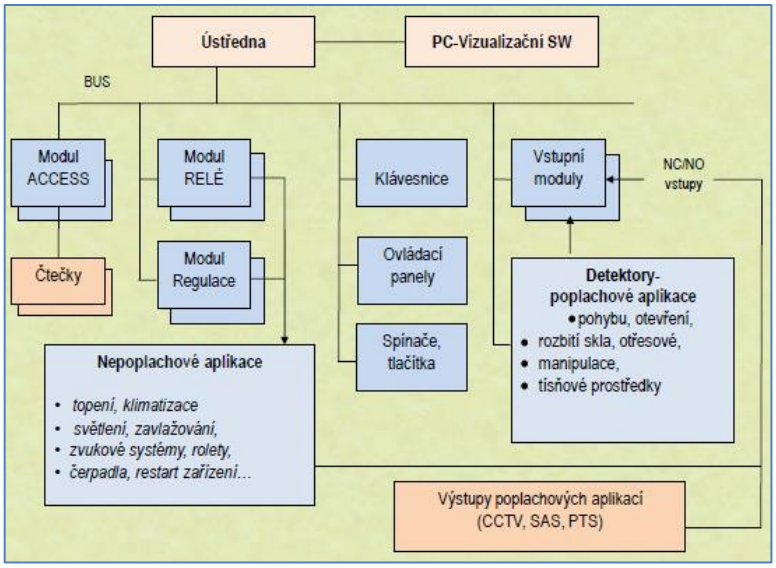


Obrázek 4: Obecné schéma HW integrace IN/OUT [6]

PZTS jako integrační prvek – modulární systémy

Modulární systémy (obecné schéma na obrázek č. 5) se využívají u rozsáhlých aplikací a obsahují speciální moduly pro ovládání například vytápění, osvětlení, klimatizace, kontroly vstupu, výtahů a průmyslových technologií. Řídící prvek je tvořen ústřednou PZTS, kdy ústředna s nadstavbovým softwarem zajišťuje komunikaci s obsluhou a ostatními prvky systému. Mezi výhody patří centrální správa informací, technologická

jednotnost komponentů a kompatibilita se softwarem. Mezi nevýhody patří centrální řízení, u něhož porucha ústředny může zapříčit nefunkčnost připojených systémů.



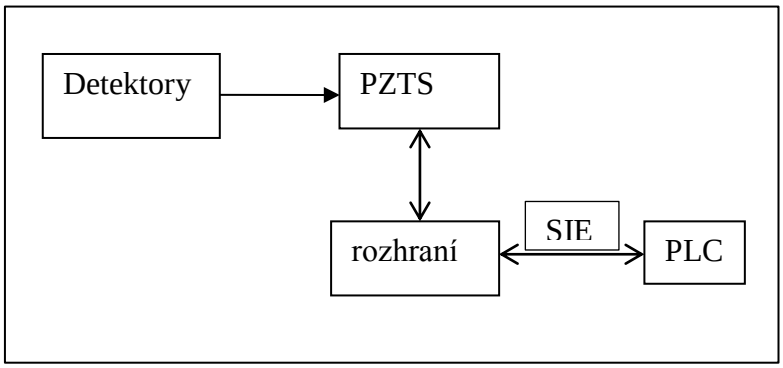
Obrázek 5: Obecné schéma HW integrace, PZTS jako ústředna modulárního systému [6]

Automatizační systém jako integrační prvek

Automatizační systémy se užívají k ovládání vytápění, osvětlení, zavlažování a k řízení jiných nepoplachových aplikací. V současné době se s pomocí integrace využívá i zabezpečení objektu. Lze naprogramovat vazby, kdy se při zastřežení vypnou světla, uzamknou dveře nebo se může spustit režim simulace přítomnosti.

Poplachový zabezpečovací systém lze připojit k systémové elektroinstalaci prostřednictvím převodníků, zajišťující oboustranný přenos signálu mezi ústřednou PZTS a řídící jednotkou systémové elektroinstalace. K ústředně je nutné připojit detektory na odděleném vedení od SIE. Samotná ústředna PZTS pak může být připojena do SIE pomocí potřebného rozhraní. Potom může být tato verze certifikována (obrázekč. 6).

Samotné automatizační moduly mohou nahradit funkci ústředny PZTS, nicméně bez této ústředny nemůže být automatizační modul certifikován.



Obrázek 6: Obecné schéma HW integrace – automatizační systém jako integrační prvek. [6]

U sběrnicových systémů se využívá komunikačních protokolů, což přináší problémy s kompatibilitou zařízení od různých výrobců, zkrátka se musí vybírat prvky tak, aby byly kompatibilní. Mezi sběrnicové systémy patří například sběrnice SIE, KNX, EIB nebo LON. [6]

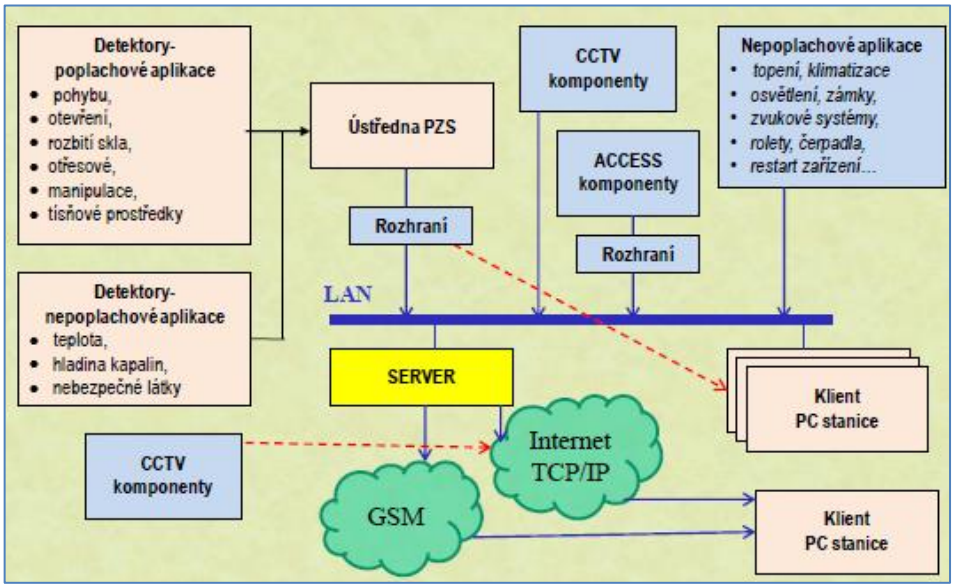
Rozhraní pro hardwarovou integraci

Mezi často používaná hardwarová rozhraní patří konektor RJ45 (obrázek č. 7), který slouží k zapojení ethernetových kabelů. Toto rozhraní se používá k připojení ústředen a dalších prvků PZTS. Dalším používaným rozhraním je RJ11(obrázek č. 7), které slouží k připojení do jednotné telefonní sítě. Rozhraní RS232 se používá pro připojení tiskáren, různých komunikátoru, rádiových vysílacích modulů apod. Konektory pro RS232 jsou D-Sub nebo DB25. Rozhraní RS485 se používá především v průmyslových odvětvích z toho důvodu, že odolávají různému rušení a lze je používat pro připojení zařízení až do vzdálenosti 1200m. U rozhraní RS484 nejsou standardizovány konektory, které mohou mít různou podobu, třeba svorkovnice. Používají se pro připojení klávesnic, koncentrátorů a detektorů. Dále se používají výstupy PGM a relé výstupy na ústřednách, ale o tom je hovořeno již o kapitolu výše. Konektory BNC (obrázek č. 7) jsou používány jako rozhraní, kdy se využívá jako vodič koaxiální kabel. Konektory ST se používají jako rozhraní u optických vláken. [6]

Obrázek 7: Konektor RJ 45, BNC a RJ11. [15]

3.6 Softwarová integrace

Softwarová integrace zajišťuje sloučení různých systémů na softwarové úrovni. To znamená, že hardwarová integrace je již dokončena a mezisystémové interakce, ovládání, správu a vizualizaci zajišťuje nadstavbový software instalovaný na serveru nebo klientském počítači. Uživatel pak v podstatě pracuje s jedním systémem, i když je tvořen různými aplikacemi. Všechny poplachové i nepoplachové aplikace mohou být připojeny k serveru prostřednictvím LAN/WAN (obrázek č. 8). U jednoduchých aplikací je propojení realizováno pomocí sériového nebo USB rozhraní.



Obrázek 8: Obecné schéma integrovaného poplachového systému propojení LAN/WAN. [6]

Funkce softwarových produktů je široká. Zahrnuje správu systémů, uživatelů, programování, monitoring, vizualizaci, ovládání, automatizaci vazeb, správu docházky, vyhodnocení událostí nebo sledování událostí. Klasifikaci softwaru můžeme rozdělit do následujících skupin: SW ústředen poplachových systémů, SW pro uživatelskou správu, vizualizační SW, Integrační SW budov.

SW ústředen poplachových systémů

Jedná se v podstatě o doplňkové programy dodávané k ústřednám určených především pro potřebu instalačních a servisních firem, které provádí konfiguraci ústředny. Pomocí tohoto softwaru lze provádět programování, sledování, vyhodnocování a archivaci událostí ústředny.

SW pro uživatelskou správu

Tyto aplikace umožňují konfigurace řídících jednotek připojených do systému. Jedná se zde hlavně o přístupové systémy a systémy kontroly vstupu. SW umožňuje nastavení uživatelských profilů, vytváření zón, časových profilů, přidělování a evidenci identifikátorů, náhled do historie apod. Pomocí těchto SW se dají také vyhodnocovat a sledovat události.

SW pro uživatelskou správu

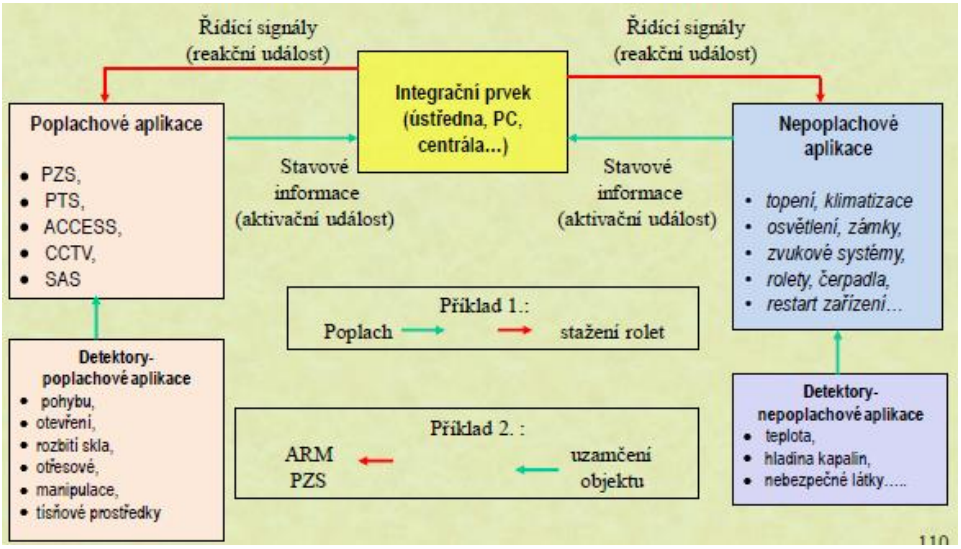
Software umožňuje vizualizaci systému v reálném čase. Pomocí vizualizačních programů, může být graficky znázorněn půdorys dané budovy, zóny nebo také perimetrická ochrana. Např. v půdoryse mohou být znázorněny kamery a jejich směrování, detektory nebo dveře, kdy můžeme například z grafického rozhraní ovládat kameru, zamykat nebo odemykat dveře, spouštět zavlažování, zastřežit nebo odstřežit objekt.

Integrační SW budov

Tento SW umožňuje propojení poplachových a nepoplachových systémů. Software je nainstalován na serveru a umožňuje nastavit automatické vazby mezi systémy, umožňuje lokální i vzdálené ovládání, realizaci vazby docházky na mzdový systém, správu systému a uživatelů atd. Aby bylo zamezeno při výpadku činnosti SW negativním interakcím mezi systémy, je nutné zabezpečit mezisystémové vazby už na HW úrovni. [6]

3.7 Funkce integrovaných systémů

Široké funkce integrovaných systémů umožňují programování nejrůznějších vazeb v systému mezi poplachovými a nepoplachovými aplikacemi. Na základě aktivační události (chování detektorů poplachových a nepoplachových aplikací) integrační prvek vyhodnotí, o jakou událost jde a vytvoří danou reakční událost (obrázek č. 9). Např. je možné naprogramovat systém tak, aby při zastřežení došlo k aktivaci detektorů, simulaci přítomnosti, zamčení všech dveří, stažení rolet, žaluzií, vypnutí el. proudu, uzavření plynu apod. Při narušení objektu může být nastavena vazba na kamerový systém, který odešle snímek nebo videosekvenci z kamery v narušené zóně na daný počítač, telefon nebo PPC. Dále může dojít při narušení ke spuštění zamlžovacích systémů. Využití integrovaných systémů je skutečně široké. [6]



Obrázek 9: Obecné schéma aktivačních a reakčních vazeb v integrovaném systému. [6]

4. LEGISLATIVNÍ A TECHNICKÉ NORMY

K realizaci a provozu výše zmíněných způsobů ochrany objektů je třeba dodržet potřebnou legislativu a technické normy. Pod legislativou se rozumí zákony a prováděcí vyhlášky, které jsou závazné. Technická norma je dokument, který obsahuje pravidla, usměrnění a charakteristiky, které slouží k dosažení určitého standardu. Úkolem technické normy je také zjednodušení a snižování rozmanitosti výrobků a činnosti a dále zavadí symboly a kódy ke zjednodušení obchodního styku. Norma také svým způsobem chrání spotřebitele. Podle obsahu existují normy například návrhové, výrobkové, prováděcí nebo jakostní. Podle územní platnosti mohou být technické normy mezinárodní, evropské a národní. V tabulce č. 3 uvedu legislativní a technické normy, které se dotýkají dané problematiky v této diplomové práci. [5]

Tabulka 3: Legislativní a technické normy

Oblast úpravy	legislativní / technická norma
Ochrana utajovaných informací	Zákon č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti
	Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznamy utajovaných informací
	Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, ve znění vyhlášky č. 453/2011 Sb.
	Vyhláška 524/2005 Sb. o zajištění kryptografické ochrany utajovaných informací
	Vyhláška č. 525/2005 Sb. o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací, ve znění vyhlášky č. 434/2011 Sb.
	Vyhláška 526/2005 Sb. o stanovení vzorů používaných v oblasti průmyslové bezpečnosti a o seznamech písemností a jejich náležitostech nutných k ověření splnění podmínek pro vydání osvědčení podnikatele a o způsobu podání žádosti podnikatele (vyhláška o průmyslové bezpečnosti)
	Vyhláška 527/2005 Sb. Vyhláška o stanovení vzorů v oblasti personální bezpečnosti a bezpečnostní způsobilosti a o seznamech písemností přikládaných k žádosti o vydání osvědčení fyzické osoby a k žádosti o doklad o bezpečnostní způsobilosti fyzické osoby a o způsobu podání těchto žádostí (vyhláška o personální bezpečnosti)
	Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb. a vyhlášky č. 454/2011 Sb.
	Vyhláška č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění vyhlášky č. 55/2008 Sb. a vyhlášky č. 433/2011 Sb.
Poplachové systémy	ČSN EN 50 130 Poplachové systémy
	ČSN EN 50 131 Poplachové zabezpečovací a tísňové systémy
	ČSN EN 50 132 CCTV sledovací systémy pro použití v bezpečnostních aplikacích
	ČSN EN 50 133 Systémy kontroly vstupů pro použití v bezpečnostních aplikacích
	ČSN CLC/TS 50 398 Kombinované a integrované systémy
	Zákon č. 101/2000 Sb., o ochraně osobních údajů (využití u kamerových systémů)
Mechanické zábranné systémy	ČSN P ENV 1627-1630, ČSN 1303,1906,12320, 1143-1,916010, 165110

DÍLČÍ ZÁVĚR TEORETICKÉ ČÁSTI

Teoretická část je rozdělena do čtyř samostatných kapitol, které na sebe navazují. První kapitola uvedla čtenáře do problematiky ochrany utajovaných informací. Je v ní rozebrána legislativa a důležité okruhy OUI jako je například fyzická bezpečnost. Pozornost byla věnována také funkci Národního bezpečnostního úřadu. Zpracování tohoto tématu bylo pro práci důležité, protože se v objektu policie budou zřizovat zabezpečené oblasti kategorie Vyhrazené a Důvěrné.

Druhá kapitola se věnuje technické ochraně, která se užívá v souvislosti s ochranou budov. V této části je čtenář obeznámen s elektrickým poplachovým a tísňovým systémem, jeho funkcí a potřebnými komponenty. Je zde také zmínka o mechanických zábranných systémech. Tato kapitola nepopisuje všechny možné komponenty ochrany, ale pouze ty, které mohou být využity k praktickému řešení úkolu.

Další část teorie byla věnována integraci bezpečnostních aplikací. Tuto kapitolu jsem zařadil do práce, protože jsem chtěl navrhnout integrovaný bezpečnostní systém, kterým policie zatím nedisponuje. V této části byl čtenář seznámen se základním rozdělením, principy a druhy integrací.

V poslední kapitole teorie jsem zmínil potřebnou legislativu a technické normy, které se dotýkají řešeného problému.

II. Praktická část

5. ANALÝZA SOUČASNÉHO STAVU OCHRANY BUDOVY POLICIE

Z bezpečnostních důvodů nebudu uvádět informace o konkrétní budově Policie ČR. Půdorysy mírně pozměním tak, aby z této práce nebylo možné odvodit, která budova je podrobena analýze a u které provedu návrh bezpečnostního řešení.

Aby mohlo být řešeno zabezpečení budovy a organizační opatření, je nejprve nutné podrobit celou budovu detailní analýze, ze které budou vycházet následná bezpečnostní řešení.

Jedná se o budovu, která je v současné době využívána jen z části a to jako policejní stanice, ale v rámci reorganizace se mají tyto prostory využívat vnější službou (obvodní oddělení), službou kriminální police a vyšetřování. Vzhledem k tomu, že zabezpečení této budovy neodpovídá současným standardům ochrany budov Policie ČR a už vůbec ne budoucím nárokům na ochranu utajovaných skutečností, je potřeba vyřešit problém se zabezpečením budovy a navrhnout odpovídající bezpečnostní řešení i v návaznosti na to, že v budově budou nově zřízeny zabezpečené oblasti v režimu vyhrazené a důvěrné.

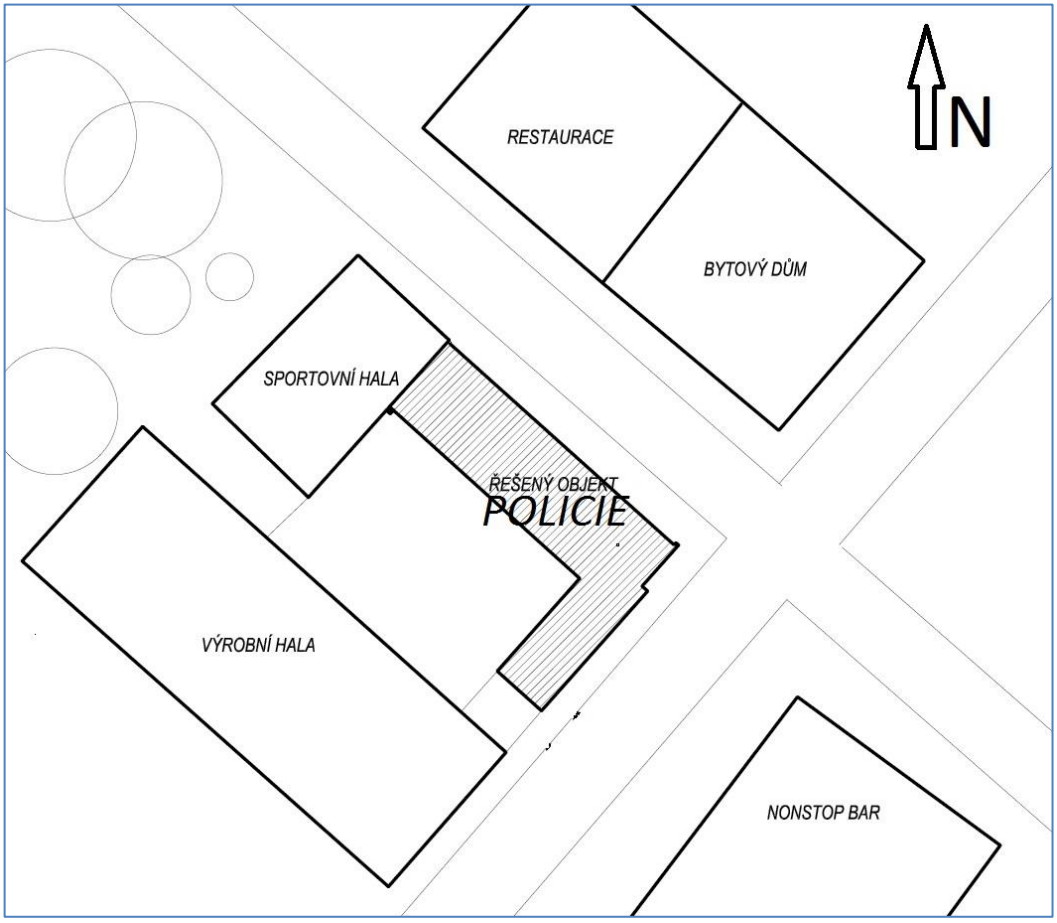
5.1 Stavebně technický popis řešené budovy

Jedná se o rohovou budovu ve tvaru písmene L. Severní křídlo budovy je trojpodlažní a východní jednopodlažní přízemní. Hranice areálu je tvořena sportovní halou a na ni navazující zdí ve výšce 2m. Dalším sousedním objektem je výrobní hala pro výrobu mléčných výrobků. Řešená budova je tvořena obvodovými zdmi cihel plných pálených tloušťky 45cm, vnitřní nosné stěny jsou tloušťky 30cm, příčky tloušťky 15cm. Objekt je založen na železobetonových pasech. Stropní konstrukce je tvořena ocelovými I profily se škvárobetonovými vložkami tloušťky 25 cm. Světlá výška místností ve všech podlažích je 2,5 m. Podlahy v místnostech tvoří především PVC, na chodbách a v sociálním zázemí je použita keramická dlažba. Vnitřní dveře jsou dřevěné s ocelovými zárubněmi. Okna byla v minulosti měněna za plastová. Objekt je vytápěn centrálním plynovým kotlem, který je umístěn v kotelně ve 2NP, tělesa ústředního topení jsou litinová, umístěná pod okny. V objektu jsou dvě schodiště z toho jedno je přístupné ze dvorní části. Schodiště jsou železobetonová s keramickou nášlapnou vrstvou. V budově je celkem 54 místností. Střecha je sedlová pokrytá pálenou taškou. Střecha má 2 průlezné otvory. Celková výška budovy západního křídla se střechou je 13,3 m a východního 6,5 m.

5.2 Umístnění stavby a analýza perimetru

Budova policie sousedí s následujícími objekty (obrázek č. 10):

1) ***Severní strana*** – naproti přes ulici se nachází restaurace a bytový dům, v jehož blízkosti je i dětské hřiště s pískovištěm a průlezkami, které navazuje na menší přiléhající park.
2) ***Východní strana*** – naproti přes ulici se nachází nonstop bar s hracími automaty a dále budovy sloužící k bydlení.
3) ***Jižní strana*** – sousedí s průmyslovým objektem pro výrobu mléčných výrobků. Tato firma pro výrobu mléčných výrobků zaměstnává asi 150 lidí s třísměnným nepřetržitým provozem. S tímto průmyslovým objektem zároveň sousedí i část dvoru objektu policie.
4) ***Západní strana*** - sousedí se stěnou sportovní haly, jejíž provoz je denně od 08 do 21 hod. S tuto sportovní halou zároveň sousedí i část dvoru objektu policie.



Obrázek 10: Situační plán řešeného objektu

Po celém obvodu objektu budovy je možno podélně parkovat a to vždy na okraji vozovky. Kolem objektu vedou dvě pozemní komunikace, ze severní a východní strany, jedná se o vedlejší vozovky, po kterých není nijak zvlášť hustý provoz.

Nonstop bar představuje jisté nebezpečí z pohledu vandalizmu, protože během posledních 5 let je evidováno 11 porušení zákona ze strany hostů tohoto baru. Další možné nebezpečí by mohlo představovat sídliště ze severní strany, které obývá asi 20 tis. obyvatel, a proto je zde i vyšší míra kriminality.

Co se týče ochrany perimetru, tak v současné době není na řešené budově žádná perimetrická technická ochrana a nejsou použity žádné kamerové systémy.

5.3 Analýza plášťové ochrany

Budova svým pláštěm, jak již bylo řečeno, přímo sdílí stěnu se sportovní halou a průmyslovou výrobnou. Budova má celkem 3 podlaží. Okna nejsou vybavena mřížemi. Do budovy je možno vejít třemi vchody – 2 vchody jsou na straně ze dvora a jeden hlavní vchod z východní ulice. Hlavním vchodem se dostaneme na recepci. Vstupy do budovy jsou chráněny dvoukřídlovými prosklenými dveřmi s plastovým rámem, vybavenými dveřním zavíračem a zámkem FAB. Dvorní trakt je přístupný také prostřednictvím průjezdu pro motorová vozidla. Tento průjezd je opatřen plechovou dvoukřídlou branou bez elektronické kontroly vstupu, se zámkem FAB. Vjezd do dvorního traktu mají povolena pouze vozidla Policie a určená vozidla. Na ochranu pláště budovy nejsou nainstalovány žádné elektrické prvky zabezpečení, plášťová ochrana je zde řešena pouze na úrovni mechanického zabezpečení kombinované s elektronickou kontrolou vstupu systémem Colnod. Tato elektronická kontrola vstupu je prováděna na recepci, v navazujícím vstupu z recepce do budovy a na vstupech do budovy ze dvora.

5.4 Analýza prostorové ochrany

Prostorová ochrana je řešena elektrickým zabezpečením. Toto zabezpečení není realizováno komplexně, ale pouze na chodbách, v dozorčí místnosti a zbrojním skladu, které jsou zabezpečeny pomocí detektorů pohybu PIR (obrázek č.11).

Obrázek 11: PIR detektory používané k prostorové ochraně.

Tyto detektory jsou připojeny k ústředně DSC typ PC 2510 CZ2 (obrázek č. 12), která je ovládána klávesnicemi DSC PC 2550RK (obrázek č. 13). Tato ústředna a klávesnice je umístěna v místnosti pro výkon dozorčí služby. Ústředna DSC PC 2510 CZ2 je dále napojena na obousměrné komunikační zařízení od firmy Fides - FA101 (obrázek č.14), které zprostředkovává obousměrnou komunikaci s ústřednou a PPC.

Obrázek 12: Ústředna DSC typ PC2510CZ2.

Obrázek 13: Klávesnice DSC PC 2550RK.

Primárně se signál předává rádiově, pomocí zařízení FA101 a k záložnímu přenosu informací slouží jednotná telefonní síť – JTS.

Toto elektrické zabezpečení bylo dle policejního oddělení technické ochrany uvedeno do činnosti asi před 20 lety a způsob, jakým je dimenzováno již neodpovídá současným standardům ochrany budov Policie.

Obrázek 14: Obousměrné komunikační zařízení od firmy Fides - FA101.

5.5 Analýza předmětové ochrany

K předmětové ochraně lze zařadit ochranu zbrojního skladu, ve kterém policisté uschovávají své služební zbraně. Zbraně jsou ve skladu uloženy v plechových uzamykatelných skříních. Ve zbrojním skladu je umístněný jeden detektor PIR a magnetický kontakt na dveřích. Vstup do místnosti je chráněn oplechovanými dveřmi

se vstupními kovanými mřížemi, které jsou uzamčeny visacím zámkem. Vedle vstupu do zbrojního skladu se nachází klávesnice pro ovládání zastřežení a odstřežení chráněné zóny. Kromě vstupních dveří není v úložně zbraní žádný další vstupní otvor.

Pro ochranu a uložení písemností je využíván trezor, který je umístěný v prostoru dozorčí služby. V budově není žádná místnost a úložný objekt pro uložení utajovaných informací.

5.6 Analýza organizačního schématu

Nyní je budova využívána jako policejní stanice, ve které slouží celkem 19 policistů pro obchůzkovou službu. Služby se střídají po 12-ti hodinových směnách. Velitelem služby je dozorčí, který dohlíží na službu v místnosti pro výkon dozorčí služby. V této místnosti se také nachází ústředna EZS a klávesnice pro obsluhu ústředny. Dozorčí rovněž vykonává ostrahu objektu. Za 12-ti hodinovou službu má za povinnost náhodně 2x zkontrolovat vnější stav budovy z venku a vnější stav budovy zevnitř – ze dvora, kdy se soustřeďuje na to, zda nebylo do budovy násilně vniknuto. V případě, že ostraha zjistí nějaké narušení chráněného objektu, učiní příslušná opatření a vyrozumí vedoucího objektu. Dozorčí má za úkol vpouštět do objektu pouze vozidla Policie přes bránu, kterou se vjíždí do dvora objektu. Rovněž zodpovídá za klíčové hospodářství. V místnosti dozorčího jsou uloženy, uzamčeny a zapečetěny všechny náhradní klíče od objektu, tyto vydává pouze osobě proti podpisu. Dozorčí rovněž zodpovídá za zbrojní sklad od kterého má klíče a provádí vydávání a uložení zbraní. O tomto pak musí udělat zápis do knihy výdeje zbraní. Do budovy je možný vstup pouze pro zaměstnance Policie, pro civilní osoby je vstup možný pouze za doprovodu příslušného policisty nebo civilního zaměstnance policie. O návštěvách ostraha objektu provádí zápis do knihy návštěv se záznamem, kdo návštěvě poskytoval oprávněný doprovod a zapíše čas příchodu a čas odchodu návštěvy.

6. NÁVRH POŽADAVKŮ NA PROJEKT ZABEZPEČENÍ BUDOVY POLICIE

Současný výchozí stav zabezpečení budovy, jak je patrné z předcházející analýzy, není optimální a nebude odpovídat požadavkům, které si níže stanovím. V řešené budově je minimální technické zabezpečení, není zde kamerový systém a žádné systémy nejsou integrovány. Po konzultaci s oddělením technické ochrany Policie, mi bylo řečeno, že pokud Policie modernizuje objekt novým technickým zabezpečením, tak ani v současné době neintegruje bezpečnostní aplikace. To například znamená, pokud Policie provádí zabezpečení svých budov, využívá k tomu PZTS, access systémy a CCTV systémy, avšak nedochází k jejich společné integraci. Vzhledem k současným trendům, technickému vývoji a klesajícím cenám techniky je chyba nevyužít integraci systémů do jedné aplikace. Proto tato práce bude také sloužit k tomu, jak by daný systém pro Policii mohl vypadat a jaké prvky by mohl obsahovat. Integrací systémů dosáhneme i vyšší úroveň zabezpečení, jednoduché správy objektu a systémů. Integrace přináší komfort pro všechny uživatele.

Za bezpečnost objektu Policie zodpovídá ředitel objektu, který si stanovuje na základě vyhodnocení bezpečnostních rizik způsob a rozsah zabezpečení. Proto zabezpečení různých budov policie může být rozdílné. V současné době se dle sdělení oddělení technické ochrany Policie zabezpečují objekty tak, že v každé místnosti je detektor pohybu a pokud není v okně mříž, tak se okenní rámy opatřují magnetickými kontakty nebo se instalují akustické detektory tříštění skla. Instalují se kamerové systémy a systémy pro kontrolu vstupu, ale jak již bylo řečeno, nedochází k integraci aplikací. Pro současný řešený objekt bude tedy požadavek, aby zmíněné aplikace byly integrovány do jednoho systému. Vytvořím náhled, jak by dané řešení mohlo vypadat a jak by bylo přibližně finančně nákladné.

6.1 Požadavky na PZTS

Řešený objekt bude zabezpečen elektrickým zabezpečovacím systémem. V každé místnosti, ve které je nějaký předmět chráněného zájmu, bude detektor pohybu. Jelikož v žádné z místností nejsou v okenních otvorech nainstalovány mříže, proto navrhuji, aby v každé místnosti přízemí (1NP) byl nainstalován akustický detektor pro detekci rozbití skleněné okenní výplně. Dále budou na chodbách vhodně rozmístěny detektory pohybu. Sociální zařízení se zabezpečovat nebudou. V budově budou nově zřizovány zabezpečené

oblasti kategorie Vyhrazené a Důvěrné a je nutné k tomu i přizpůsobit a použít techniku, která je certifikovaná od NBÚ a dále navrhnout takové prostředky, aby byly splněny bodové požadavky zabezpečených oblastí dle dané vyhlášky. Tyto zabezpečené oblasti „V“ a „D“ budou mít u vstupu klávesnice pro odsřežení a zastřežení dané oblasti. Ostatní zabezpečené úseky, např. oddělení se budou zastřežovat a odstřežovat na základě dat z přístupového systému, kdy při vstupu do určité zóny dojde k odstřežení a při odchodu posledního pracovníka dojde k zastřežení.

6.2 Požadavky na elektronickou kontrolu vstupu

Po celém objektu bude monitorován a logován pohyb osob tak, aby mohlo dojít na základě vyhodnocení informací z elektronické kontroly vstupu k zastřežení či odstřežení příslušné zóny. Zároveň budou nastaveny v systému práva tak, aby do jednotlivých úseků a oddělení, měli přístup jen daní zaměstnanci. Jednotlivá oddělení a pracovní úseky budou opatřeny kontrolou vstupu. Kontrola vstupu bude prováděna do každé zóny. Vstup se bude ověřovat rovněž na všech vstupech do budovy kromě recepce. Volný vstup na recepci bude možný v pracovní době od 07:00 do 18:00, kdy je zde přítomen recepční, mimo tuto dobu se venkovní vstupní dveře automaticky uzavřou a vstup na recepci bude možný pouze na základě autorizace přes čtečku služebních karet. Zároveň budou vstupní dveře z recepce dále do budovy vybaveny kontrolou vstupu tak, aby se nepovolaná osoba nedostala do objektu. Nově bude ověřován i vjezd do dvorního traktu, kdy bude potřeba nahradit současná dvoukřídlá ocelová vrata automatickými rolovacími, kdy na základě vyhodnocení dat ze čtečky služebních karet dojde k jejich otevření.

6.3 Požadavky na kamerové systémy

Pro monitoring perimetru by měly být užity jak PTZ kamery, tak statické kamery. PTZ kamery budou umístěny tak, aby pokryly celý perimetr. Statické kamery budou umístěny tam, kde je potřeba nepřetržitý monitoring, např. na recepci u vstupu do budovy, vjezdu do areálu a k nepřetržitému monitorování policejních cel pro zadržené osoby. Vzhledem k tomu, že v současné době se stávají díky pokročilému technickému vývoji a stále klesajícím cenám standardem digitální IP kamerové systémy, bude tento projekt řešen výhradně na platformě IP. Při dnešních cenách by bylo nerozumné investovat do analogových kamer, které jsou již technologicky překonány. Kamerový systém bude integrovaný k access systému, kdy integrovaný systém provede obrazový záznam události

vstupu nebo výstupu osoby z budovy. Mezi kamerovým systémem a access systémem tedy bude vazba.

7. NÁVRH TECHNICKÉHO ZABEZPEČENÍ BUDOVY

V této kapitole se budu zabývat návrhem technického zabezpečení budovy. Techniku budu volit tak, aby veškeré bezpečnostní systémy byly integrovány do jednoho kompaktního celku. Policie takové řešení ještě nemá, tak se pokusím vytvořit návrh, jak by takové řešení mohlo vypadat a zkusím také odhadnout, jak by bylo finančně nákladné. V požadavcích na zabezpečení budovy Policie, které jsem navrhl, budu integrovat bezpečnostní aplikace typu elektronického zabezpečení, kontroly vstupu do budovy a kamerové systémy.

Protože Policie pracuje i s utajovanými informacemi, je nutné k tomu i přizpůsobit prostředí, zřídit zabezpečené oblasti. V této části diplomové práce navrhnu také prostředky nutné pro zabezpečené oblasti kategorie Důvěrné a Vyhrazené tak, aby bylo dosaženo zákonem požadovaného minimálního bodového ohodnocení pro kategorii Důvěrné s určenou mírou rizika. Součástí budou i cenové náklady na komponenty nebo výrobky, které jsou nutné ke zřízení zabezpečených oblastí.

7.1 Zabezpečení budovy integrovaným systémem na bázi VAR-NET INTEGRAL

Řešení od firmy VARIANT plus s.r.o. nabízí kompletní integraci poplachových a nepoplachových aplikací na bázi VAR-NET INTEGRAL. Třebíčská firma VARIANT plus byla založena v roce 1992 a je zaměřena na velkoobchodní činnost v oblasti bezpečnostních a dalších elektronických systémů. V minulých letech začala firma nabízet komponenty pro bezpečnostní průmysl pod vlastní značkou VAR-TEC. Jde například o prvky perimetrické ochrany, požární detektory, detektory plynu, kabely akumulátory apod. Firma nabízí i docházkový systém VAR-NET určený pro menší a střední firmy (až 200 zaměstnanců). Počátkem roku 2011 firma rozšířila zastoupení o obor integrace systémů budov. V rámci toho nabízí i nový SW VAR-NET INTEGRAL, který umožňuje integrovat bezpečnostní systémy a jiné např. průmyslové aplikace. [17]

7.1.1 PZTS

Poplachový systém bude v budově instalován tak, že ústředna bude umístěna v prostorech výkonu dozorčí služby, která vykonává i ostrahu objektu. V této místnosti bude i vnitřní akustická signalizace. Venkovní zvuková signalizace bude umístěna na zdi budovy na venkovní stěně a na stěně budovy z dvorního traktu. Akustické detektory rozbití skla budou instalovány v kancelářích v přízemí budovy. Detektory pohybu budou instalovány ve všech místnostech a na chodbách. PZTS bude dimenzován pro míru rizika střední tak, aby vyhovoval certifikaci NBÚ 2 stupně, tedy pro ochranu utajovaných informací kategorie Důvěrné. Návrh zabezpečení, rozmístění prvků PZTS a definice bezpečnostních zón je vyobrazeno v grafické příloze této diplomové práce a to pod označením P4-P7.

Ústředna Paradox Digiplex EVO 192 + BOX VT

Jedná se o ústřednu pro rozsáhle objekty (obrázek č. 15), která nabízí až 192 zón. Systém umožňuje instalovat klasické drátové zóny připojené přes expandéry (1 expandér má 16 zón). Je možné připojit BUS detektory a bezdrátové detektory. Na desce ústředny je 5 PGM výstupů. Uživatel může systém ovládat klasicky přes klávesnici, pomocí bezdrátových klíčenek, přes čtečku kartami nebo přes čtečku otisku prstů. Ústředna má integrovanou nadstavbu přístupu, která umožňuje pomocí čteček a karet řídit pohyb osob po objektu. Komunikace je možná přes IP nebo GSM. Počet modulů připojených ke sběrnici může být až 254. Základní technické vlastnosti ústředny jsou uvedeny v tabulce č. 4. Orientační cena je asi 5.500,- Kč bez DPH. [17]

Obrázek 15: Ústředna Paradox EVO 192. [17]

V následující tabulce č. 4 jsou uvedeny základní technické vlastnosti ústředny Paradox EVO 192. K ústředně je nutné pořídit záložní napájení - např. AKKU SMART 12V/26Ah. K ústředně se v případě potřeby připojují expandéry, např. Paradox ZX8, který obsahuje 8 vstupů. [17]

Tabulka 4: Základní technické vlastnosti ústředny Paradox EVO 192. [17]

Max. počet zón v systému:	192
Max. počet modulů v systému:	254
PGM výstupy na ústředně:	4 x opto-relé 50 mA polarita +/- 1 x relé 5 A, 24 V
Historie událostí:	2048
Napájení:	16 V~, 40 VA
Změna firmware:	ano, pomocí software WinLoad
Zobrazení historie událostí:	software WinLoad
Doporučený záložní akumulátor:	12 V, 7 Ah/18 Ah
Max. počet zón na desce ústředny:	16
Zónový expandér:	ano, 16 zón jeden expandér
Sběrnicové detektory:	ano
Bezdrátové zóny:	ano, přijímač/vysílač RTX3
Max. počet keyswitch vstupů:	32
Max. počet PGM výstupů v systému:	250
Bezdrátové PGM výstupy:	ano, s přijímačem RTX3
Uživatelské kódy:	998
Délka uživatelského kódu:	4 nebo 6-místný
Možnost ovládání systému:	uživatelským kódem, kartou,bezdrátovou klíčenkou, keyswitchem,softwarem NEWARE, WinLoad,web prohlížečem - IP100,dálkově po telefonní lince VDMP3
Automatické zapnutí:	ano, podle času, klidu v systému
Typy zapnutí:	úplné, FORCE, STAY
Max.počet monitorovaných dveří/čteček:	32
Počet držitelů karet:	999
Způsob ovládání přístupové nadstavby:	kartou, klíčenkou, kódem
Klávesnice:	K641,K07C, K656
Software:	WinLoad
NEWARE SECURITY:	uživatelská správa EZS
NEWARE ACCESS:	uživatelská správa ACCESS/EZS

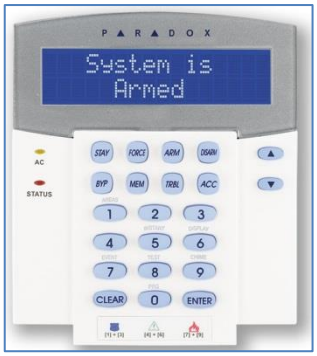
Ústředna Paradox Digiplex EVO 192 vlastní certifikát od NBÚ pro střední až vysoké riziko a dosahuje bodového ohodnocení SS91 = 3 body (Tabulka. č. 5).

Tabulka 5: Informace o certifikátu uděleným NBÚ pro ústřednu Paradox EVO 192. [7]

Identifikační číslo TP	Název výrobku	Popis výrobku	Výrobce jméno	Držitel jméno	Počet bodů dle BS	doba platnosti
T1142/2012	Ústředna EZS s bezdrátovou nástavbou	DIGIPLEX EVO 192	PARADOX SECURITY SYSTEMS	VARIANT plus, spol. s r.o.	SS91=3, SS91=2 (při použití radiového systému)	9.8.2015

Klávesnice Paradox K641

Tato klávesnice (Obrázek č. 19) je kompatibilní s ústřednami Digiplex EVO 192. Disponuje dvouřádkovým LCD displejem pro zobrazení informací o stavu ústředny, stavu zón nebo může na displeji zobrazit historii událostí ústředny. Technické informace o klávesnici K641 jsou uvedeny v tabulce č. 6. Orientační cena asi 2.600,- Kč bez DPH. [17]



Obrázek 16: Klávesnice Paradox K641

Tabulka 6: Základní technické vlastnosti klávesnice K641. [17]

Typ klávesnice:	LCD
Kompatibilita:	EVO192
Použití v systému:	ovládací, programovací
Dokumentace:	Instalační manuál – DIGIPLEX klávesnice Uživatelský manuál – EVO a K641 LCD
Adresace klávesnice v systému:	jedinečné číslo SN
Jazyková verze:	česká
Napájení:	11 - 16 V=
Proudový odběr:	min. 80 mA, max. 120 mA
Firmware:	uložen v EEPROM paměti
Displej:	dvouřádkový, 32 znaků, podsvícený
Barva displeje:	modrá
Nastavení parametrů displeje:	podsvit, kontrast, rychlost přepisu
Programování klávesnice:	na klávesnici nebo WinLoad
Klávesová zóna:	ano, 1
Typ zóny na klávesnici:	NC, bez hlídáním tamperu
Programovatelný výstup PGM:	ano, 1, max. zatížení 50 mA
Zobrazování stavu systému:	na LCD displeji
Zobrazování stavu zón:	na LCD displeji
Indikace připraveno/zapnutí:	zelená/červená LED dioda
Indikace napájení AC:	žlutá LED dioda
Prohlížení historie událostí:	ano

Detektor pohybu DM60 BUS detektor QUAD

Jedná se o PIR detektor s plně digitálním zpracováním signálu (obrázek č. 17) s připojením na sběrnici BUS, po které obousměrně komunikuje. Signál ze senzoru jde do převodníku A/D, pak následuje digitální zpracování v procesoru a spektrální analýza. Tento detektor bude použit pro běžné zabezpečení místnosti a chodeb, které nejsou součástí zabezpečených oblastí pro ochranu utajovaných informací. Základní technické údaje jsou uvedeny v tabulce č. 7. Orientační cena asi 800,- Kč bez DPH

Obrázek 17: Detektor pohybu DM60 BUS detektor QUAD. [17]

Tabulka 7: Základní technické vlastnosti pohybu DM60 BUS detektor QUAD. [17]

Typ detektoru:	digitální na BUS sběrnici
Kompatibilita:	EVO192 Univerzální kloubový stojan - SB469 Výměnné čočky LR-1, LR-2, LR-3, LR-4, WA-2, WA-3, WA-4, PE-1, CU-1
Senzor:	quad
Dokumentace:	Instalační manuál - DIGIPLEX moduly BUS
Adresace detektoru v systému:	jedinečné číslo SN
Nastavení detektoru:	software WinLoad z PC
	klávesnice - instalační programování
Napájení:	11 - 16 V=
Proudový odběr:	min. 13 mA, max. 24 mA
Odolnost na elektr. pole:	10 V/m
Montážní výška:	2 - 2,7 m
Dosah:	12 m, 110° standardní čočka WA1
Poplachový výstup:	po BUS sběrnici
Tamper výstup:	po BUS sběrnici /podle nastavení/
Detekční rychlost:	0,2 až 3,5 m/s
Optická indikace:	červená LED dioda
Barva krytu:	bílá

Detektor pohybu DOUBLE-TEC PIR+MW, AM

Jedná se o duální detektor pohybu PIR + MW (obrázek č. 18). Detektor je vybaven funkcí antimasking. Detektor bude použit pro zabezpečení zabezpečených oblastí kategorie Důvěrné, Vyhrazené a částí budovy, kde hrozí rušení z vnějšího prostředí. Technické parametry jsou uvedeny v tabulka č. 8. Tento detektor má certifikaci od NBÚ - SS91 = 3 body (tabulka č. 9). Orientační cena asi 1.000,- Kč bez DPH.

Obrázek 18: Detektor pohybu DOUBLE-TEC PIR+MW, AM. [17]

Tabulka 8: Technické parametry Detektor pohybu DOUBLE-TEC PIR+MW, AM. [17]

Typ detektoru:	digitální PIR + MW
Vznik poplachu:	režim AND nebo OR
Antimasking:	ano
Citlivost:	samostatně citlivost PIR a MW
Napájení:	8 - 16 V=
Proudový odběr:	25 mA
Montážní výška:	1,8 - 2,2 m
Dosah:	12 m, 110°
Poplachový výstup:	NC, 24 V=, 100 mA
Tamper výstup:	NC, 24 V=, 100 mA
Detekční rychlost:	0,1 až 5 m/s
Optická indikace:	LED dioda

Tabulka 9: Informace o certifikátu detektoru pohybu DOUBLE-TEC PIR+MW, AM. [7]

Identifikační číslo TP	Název výrobku	Popis výrobku	Výrobce jméno	Držitel jméno	Počet bodů dle BS	doba platnosti
T1088/2012	Kombinovaný detektor PIR+MW, AM	DOUBLE-TEC	MAXIMUM ELECTRONICS LTD.	VARIANT plus, spol. s r.o.	SS91=3	9.8.2015

Akustický detektor rozbití skla DG457 GLASSTREK

Tento detektor (obrázek č. 19) analyzuje tlakovou vlnu vzniklou prolomením skleněné plochy a dále analyzuje akustické tříštění skla. Detektor je adresný, připojuje se přímo ke sběrnici a lze ho provozovat ve dvou režimech citlivosti (4,5 nebo 9m). Tento detektor bude použit k zabezpečení běžných neutajovaných místností v přízemí. Orientační cena asi 700,- Kč bez DPH.

Obrázek 19: Akustický detektor rozbití skla DG457 GLASSTREK. [17]

Akustický detektor Honeywell FG1625TAS

Tento detektor bude použit pro zabezpečené oblasti kategorie Důvěrné a Vyhrazené. Výrobek má certifikaci od NBÚ, který mu udělil S91 = 2 body (Tabulka č. 10). Orientační cena asi 750,- Kč bez DPH.

Tabulka 10: Informace o certifikátu detektoru rozbití skla Honeywell FG1625TAS. [7]

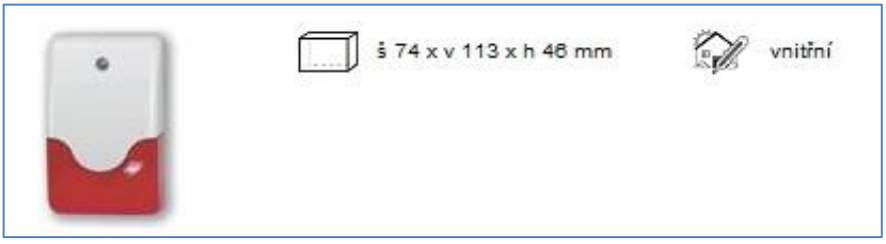
Identifikační číslo TP	Název výrobku	Popis výrobku	Výrobce jméno	Držitel jméno	Počet bodů dle BS	doba platnosti
T1016/2013	Detektor rozbití skla	FG1625TAS	Honeywell International Inc.	Honeywell International Inc.	SS91=2	12.12.2015

Tabulka 11: Technické parametry detektoru rozbití skla Honeywell FG1625TAS. [17]

Typ detektoru	duální detektor tříštění skla
Napájení	6 - 18 V
Proudový odběr (klid / max)	13/22mA
Dosah	7,6m max.
Minimální rozměr skla	28 cm2

Signalizace vnitřní - SA913

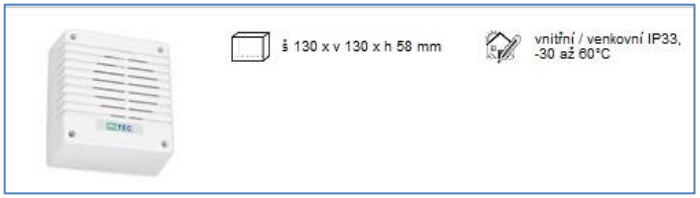
Jedná se o vnitřní akustickou a optickou signalizaci (obrázek č. 20). Tato piezosiréna dosahuje 110 dB/m akustického výkonu. Předepsané napájení je 11-14V a proudový odběr je 250mA. Tato signalizace bude nainstalována u dozorčího. Orientační cena asi 230,- Kč bez DPH.



Obrázek 20: Signalizace vnitřní - SA913. [17]

Signalizace venkovní BELL-TEC SIREN

Tato venkovní akustická signalizace (obrázek. č. 21) bude umístěna na plášti budovy z venkovní strany a druhá ze dvora. Jedná se o magnetodynamickou akustickou signalizaci o výkonu 105 dB/m. Předepsané napájení 10-14 V, proudový odběr 400 mA. Orientační cena asi 430,- Kč bez DPH.



Obrázek 21: Signalizace venkovní BELL-TEC SIREN. [17]

7.1.2 Přístupový systém

Součástí ústředny Paradox Digiplex EVO 192 je i možnost použití access nadstavby. Touto nadstavbou je možné do systému zařadit čtečky a ty využívat k zastřežení a odstřežení dané zóny a samozřejmě také řídit pohyb osob po objektu. Pro využití těchto funkcí je nutné osadit dveře čtečkou karet pro autorizaci vstupu a modulem pro vytvoření přístupového bodu. Tento modul pak ovládá elektromagnetický zámek dveří.

Návrh rozmístění prvků ACCESS je vyobrazen v grafické příloze této diplomové práce a to pod označením P4-P7.

ACCESSPACK 910-ACM12+R910

Pro vytvoření přístupového bodu lze využít balík ACCESSPACK 910-ACM12+R910 (obrázek č. 22) určený ústřednám EVO 192. Tento nadstavbový balík obsahuje modul pro vytvoření přístupového bodu. Modul se připojí po sběrnici k ústředně EVO 192. Součástí balíku jsou i dvě čtečky karet R910 pro venkovní a vnitřní použití, kterými se osadí dveře na obou stranách. Modul je nutné uložit např. do Boxu M-40, který obsahuje i napájení. Technické parametry modulu ACM12 jsou uvedeny v tabulka č.13, technické parametry čtečky v tabulka č. 12. Orientační cena asi 4.700,- Kč bez DPH.

Obrázek 22: Proximity čtečka Paradox R910 s access modulem ACM12. [17]

Tabulka 12: Technické parametry čtečky karet Paradox R910 . [17]

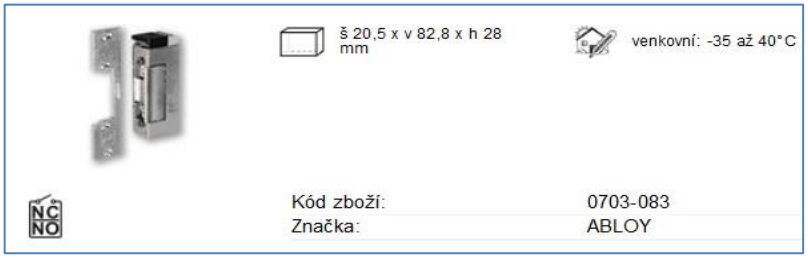
Typ modulu:	bezdotyková čtečka
Kompatibilita:	ACM12 C702/C704/RAC1/RAC2/C706
Typ čtečky:	PROXIMITY
Čtecí dosah:	8 cm
Karta:	PROXIMITY karta PARADOX
Frekv. budícího pole čtečky:	125 kHz
Výstupní formát:	RS-485
Max. vzdálenost od modulu přístupu:	300 m, 4 dráty
Optická signalizace:	červená/zelená LED dioda
Audio signalizace:	ano, bzučák

Tabulka 13: Technické parametry access modulu ACM12. [17]

Typ modulu:	modul přístupu + zdroj
Adresace modulu v systému:	jedinečné číslo SN
Kompatibilita:	Ústředna - EVO192 Čtečky - R870, R910, R915 Čtečky jiných výrobců - Wiegand 26 bit
Vstup pro čtečku:	ano, 1 vnitřní/venkovní čtečku RS485
Napájení:	16 V~, 40 VA
Doporučený záložní akumulátor:	12 V, 7 Ah/18 Ah
Proudový odběr modulu:	max.80 mA
Počet vstupů/zón:	2, zóna CT (magnet), REX (detektor)
Tamper vstup:	ano, NC tamper modulu
Programovatelný výstup PGM:	ano, 1 x tranzistor 50 mA
Výstup pro otvírání dveřního zámku:	ano, 1 x relé
Doporučený typ boxu:	BOX M-40, BOX S-40, BOX VZ-40

Elektromechanický zámek dveří 17RR-E4

Tento zámek (obrázek č. 23) s monitorováním stavu dveří se instaluje do zárubně nebo nepohyblivé části dvoukřídlích dveří. Po přivedení napětí se západka uvolní a pak je možné dveře otevřít, po odpojení napětí je zámek opět blokován. Napájení 12V, proudový odběr 270 mA, výstupní kontakty NO/NC. Orientační cena asi 1.200,- Kč bez DPH.



Obrázek 23: Elektromechanický zámek 17RR-E4. [17]

Kabeláž

Pro kabeláž byl firmou Variant doporučen kabel VL 06-6 x 0,22. Který má 4 měděné žíly a plášť z PVC. Stínění je realizováno Al folií. Prodává se ve 100 m balení přibližně za 500,-Kč bez DPH.

7.1.3 Kamerový systém CCTV

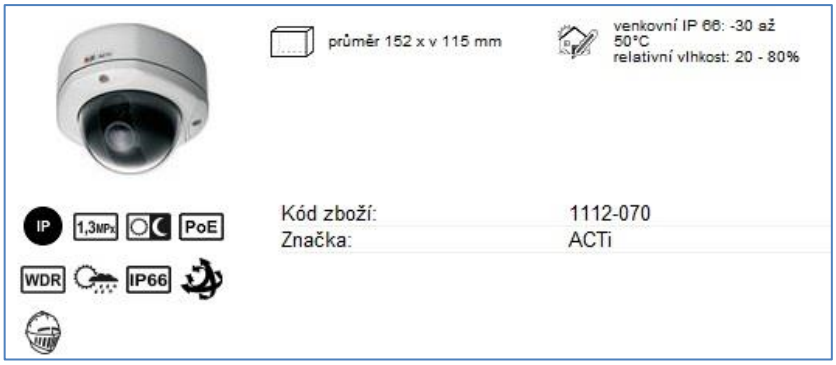
Kamerový systém bude postaven výhradně na IP technologii. U řešení od firmy Variant není třeba dokupovat IPCordery. O záznam obrazu se stará integrační server připojený do sítě LAN (více v kapitole 7.1.4). Celkem bude použito 10 statických kamer a 2 kamery PTZ. Všechny budou pro venkovní použití. Tři statické kamery v provedení antivandal budou instalovány pro monitoring tří policejních cel. Ostatní kamery budou připevněny na plášť budovy tak, aby monitorovaly vchody do budovy a plášť budovy. Kamery budou zapojeny do datového rozvaděče switch s PoE napájením.

Aby bylo možné kamerový systém integrovat s ostatními bezpečnostními aplikacemi, je nutné vybírat kamery značky ACTi nebo Canon, pro které má firma Variant napsané drivery. [18]

Návrh rozmístění kamer je zobrazen v grafické příloze s označením P8.

Kamera pro monitoring policejní cely ACTi TCM-7411

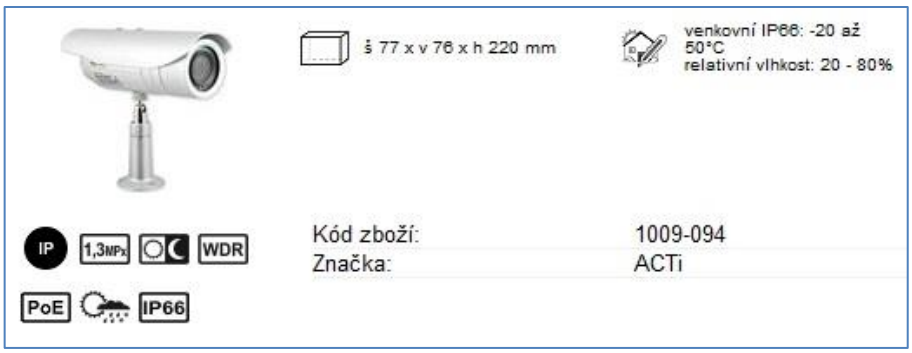
Jedná se o 1,3Mpx IP kameru v provedení antivandal (Obrázek č. 24), která bude použita pro monitoring policejních cel. Maximální rozlišení kamery je 1280 x 1024 px - 18 sn/s, při rozlišení 1280 x 720 kamera snímá rychlostí 26 sn/s. Umožňuje kompresi videa kodeky H264, MPEG4, MJPEG. Napájení PoE dle normy 802.3af, 48V, spotřeba 4W. Připojení do sítě ethernet (100 Mbit/s) je možné přes RJ45. Datový tok 3-5 Mbit. Orientační cena 11.400,- Kč bez DPH. [17]



Obrázek 24: IP kamera ACTi TCM-7411. [17]

Kamera ACTi TCM-1231 pro snímání pláště budovy a vstupů do budovy

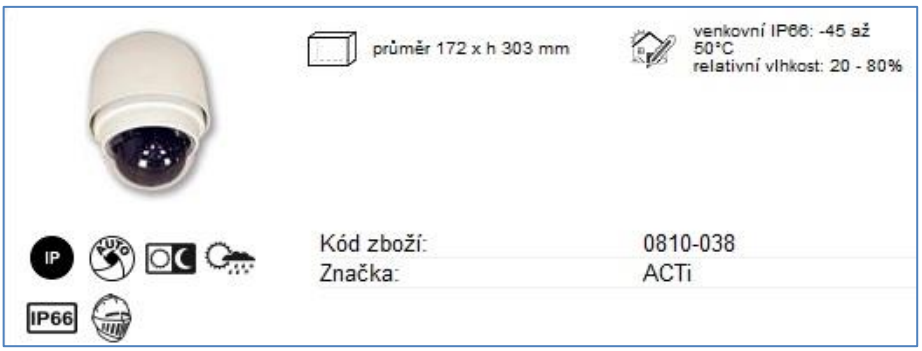
Tato externí 1,3Mpx IP kamera (Obrázek č. 25) bude použita pro snímání pláště budovy z venkovní strany a všech vstupů do budovy. Maximální rozlišení 1280 x 1024 px pro 18 sn/s, při rozlišení 640 x 480 kamera snímá rychlostí 30 sn/s. Komprese kodeky H264, MPEG4, MJPEG, napájení pomocí PoE dle normy IEEE 802.3af, připojení do sítě ethenet pomocí RJ45, kamera disponuje IR přísvitem (30 m) - pracuje v režimu den/noc. Spotřeba 8 W. Datový tok 3-5 Mbit. Orientační cena 12.200,- Kč bez DPH. [19]



Obrázek 25: IP kamera ACTi TCM-1231. [17]

PTZ SpeedDome kamera ACTi CAM-6630P

Tato kamera bude použita pro monitoring perimetru. Rozlišení kamery je 720 x 576 px při 25 sn/s. Kamera disponuje 35x optickým zoomem, rozhraní pro připojení do sítě ethenret je standardní RJ45. Napájení 24V, spotřeba 65W. Komprese je prováděna kodeky MPEG-4. Kamera podporuje režim den/noc. Datový tok 3-5 Mbit. Orientační cena 52.000,- Kč bez DPH. [19]



Obrázek 26: IP kamera ACTi CAM-6630P . [17]

K ovládání PTZ kamery se pak použije Joystick, kdy postačí jakákoli základní verze, u které se cena pohybuje okolo 6.000,- Kč bez DPH.

7.2 Integrační HW

K tomu, aby bylo možné všechny dané aplikace integrovat do jednoho kompaktního celku, bude potřeba nad jednotlivými bezpečnostními aplikacemi použít další hardware a software. Po hardwarové stránce se bude jednat o různé převodníky, servery atd. Po softwarové stránce se bude jednat o serverový OS, různé integrační sw nadstavby atd.

7.2.1 Hardware potřebný k realizaci integrace bezpečnostních aplikací

V našem případě bude potřeba následující hw vybavení:

1) **Server**

   Dodavatel integračního řešení doporučuje následující min. HW požadavky pro systém s připojenými 16ti IP kamerami: CPU - Intel Core 2 Quad 2,5GHz, RAM min. 4GB, síť 1GBit, HDD 2 TB na týden záznamu z kamer. Navrhuji použít následující řešení serveru od firmy DELL.

   DELL PowerEdge T110 II

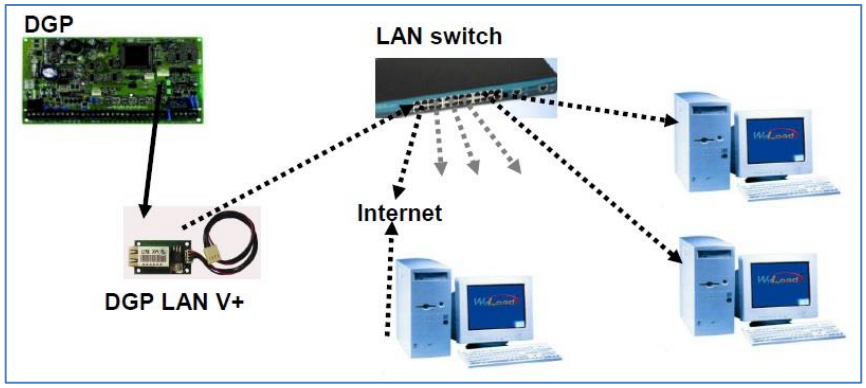
   - CPU - Intel Xeon E3-1220, 3,1 GHz (4 jádro)
   - RAM – 8 GB

- SÍŤ – 2 x 1 GBit
- HDD – 2 x 1 TB v poli RAID 1

Orientační cena serveru je 25.000,- Kč bez DPH. Pro vyšší kapacitu HDD je možno zaměnit disky za 2 kusy 2 TB, které budou zapojeny v poli RAID 1. [19]

2) **Převodník TCP/IP**

Aby mohl server pracovat s ústřednou Digiplex EVO 192 po síti LAN, je potřeba připojit k ústředně převodník TCP/IP. K tomuto převodu se využívá převodník **DGP LAN V** + (Obrázek č. 27). Tento převodník se připojí do konektoru ústředny SERIÁL I/O (4 pinový kabel), ze kterého je i napájen. Rozhraní pro připojení do sítě LAN je RJ45. Převodník je využíván programy WinLoad, Neware a Varnet-integral ke komunikaci s ústřednou. Na počítači, na kterém běží výše zmíněný software, musí být nainstalován sw redirector. Redirector vytvoří zpět ze sítě LAN virtuální port COM. Cena převodníku je 3.400,- Kč.



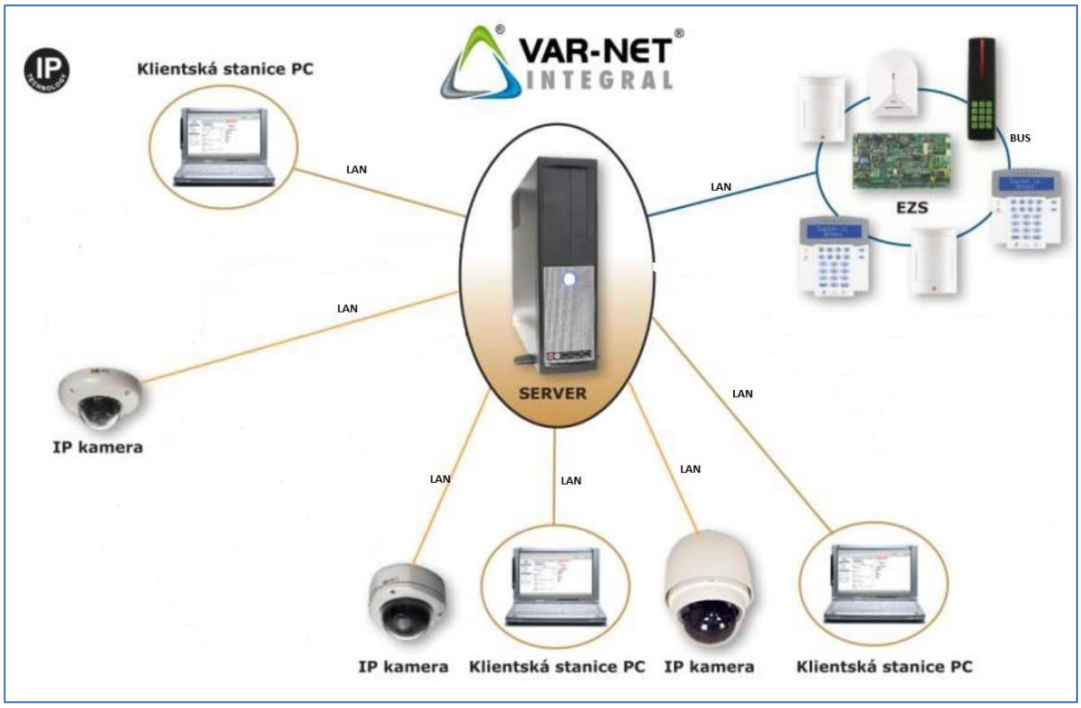
Obrázek 27: Blokové schéma zapojení ústředny do sítě LAN přes převodník. [17]

3) **Switch pro připojení IP kamer**

Pro připojení IP kamer lze použít switch PoE, switch Micronet 24/24+2 MN. Tento switch disponuje 24 porty RJ45 10/100 Mbps, kdy může napájet síťová zařízení pomocí PoE. Maximální proudový odběr na port je 15,4 W, proto je tento switch vhodný pro připojení navrhovaných IP kamer do sítě ethernet. Pro připojení do páteřní sítě disponuje switch dvěma 1Gbit FX porty. Konstrukční provedení tohoto switche je určeno pro umístnění do rack skříně. Orientační cena asi 12.800,- Kč bez DPH. [20]

Na obrázku č. 28 je znázorněno výsledné blokové schéma zapojení poplachových aplikací, kdy je do sítě LAN připojen server (tvoří hlavní integrační prvek), IP kamery, PC klienti,

ústředna EVO 192 prostřednictvím převodníku DGP LAN +. K této ústředně jsou po sběrnici připojeny detektory, klávesnice a moduly access přístupových bodů se čtečkami karet. Přesné a podrobnější blokové schéma navrhovaného řešení je v příloze DP pod označením P9.



Obrázek 28: Obecná schéma hardwarové integrace bezpečnostních aplikací. [18]

7.3 Integrační SW

Pokud je vyřešena hardwarová integrace je na řadě aplikovat softwarové řešení, které bude funkčně integrovat bezpečnostní aplikace.

Aby mohlo být využito integrační řešení Var-net Integral, je nutné, aby byla na serveru nainstalována min. verze OS Windows Web Server 2008 SP1, na které bude běžet Micosoft IIS a MS SQL. Orientační cena výše jmenovaného OS je asi 6.000,- Kč bez DPH.

7.3.1 VAR-NET INTEGRAL

Jedná se o komplexní softwarový nástroj pro správu, kontrolu a ovládání bezpečnostních a jiných elektronických systémů budov. Podporuje integraci PZTS, CCTV, EPS, ENVIRO. Instalace bezpečnostních systémů má přímou vazbu na integrační software VAR-NET INTEGRAL. Systém je plně modulární a umožňuje zvolit pouze potřebné funkce a moduly. Lze využít tyto moduly:

- Vizualizace
- Dispečink (on-line monitoring)
- Docházka
- Recepce
- Správa uživatelů

Software běží na straně serveru. Jedná se o architekturu klient – server. Klient přistupuje k systému pomocí webového prohlížeče. Všechna data jsou umístěna v jedné společné databázi a klient tedy přistupuje vždy k aktuálním informacím. Databáze obsahuje data k osobám, logy všech událostí ze všech připojených systémů, zaznamenávají se všechny uživatelské přístupy a ovládání.

7.3.2 Funkce VAR-NET INTEGRAL nad ústřednou EVO 192 (PZTS + ACCESS)

- Software monitoruje a zobrazuje on-line stav ústředny. Zobrazuje například narušení zóny, zapnutí, vypnutí podsystému, poplach, použití karty atd.
- Software ovládá ústřednu – zastřeženo /odstřeženo, otevírání zámků v přístupovém systému.
- Nahrává do ústředny uživatelské oprávnění (PIN, karty, oprávnění na podsystémy – dveře, oprávnění uživatele atd.)

7.3.3 Jednotlivé moduly SW VAR-NET INTEGRAL – licence

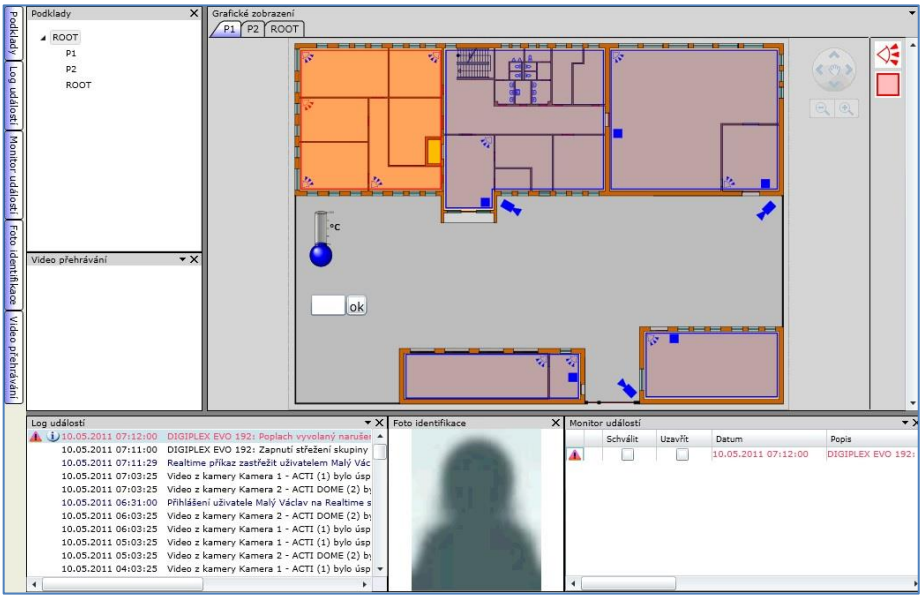
Celý systém VAR-NET INTEGRAL, jak již bylo řečeno, je modulární a lze využívat jen okruhy a moduly, které skutečně potřebujeme. Samotné řešení již obsahuje základní jádro a základní licence, které lze využívat. Pokud by se jednalo o rozsáhlejší objekt, je nutné další licence a moduly přikoupit

Základní jádro systému tvoří: základní číselníky, správa logů, licence pro jeden připojený okruh, neomezený počet SW klientů (práce ve webovém prohlížeči). Maximální počet okruhů je 6. Cena jádra (jeden okruh) sw VAR-NET INTEGRAL je 5.000,- Kč bez DPH.

Okruhy a moduly VAR-NET INTEGRAL, které budou využity

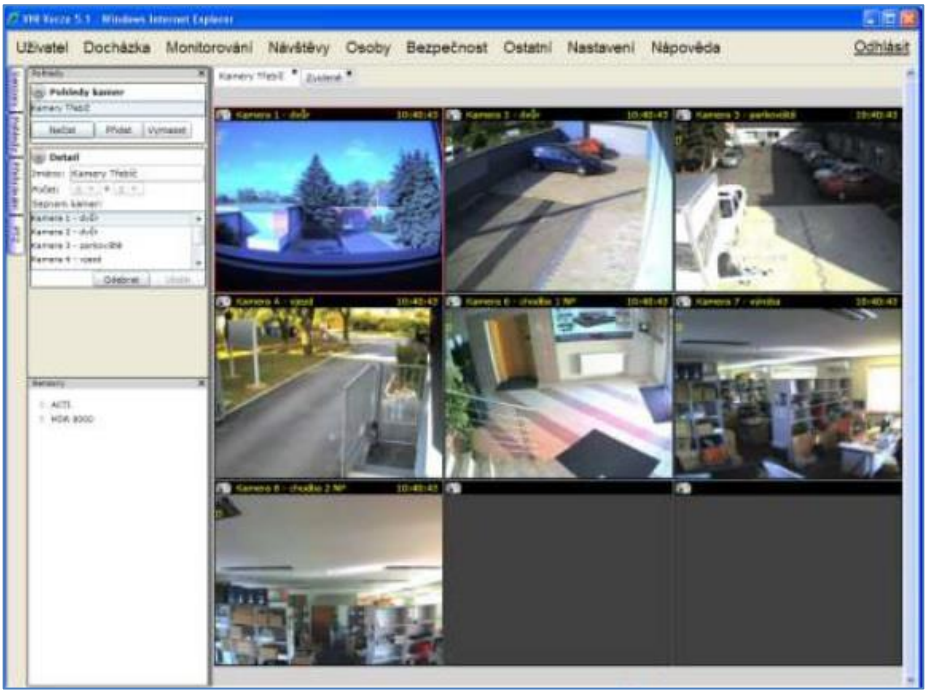
- PZTS je okruh pomocí kterého se v systému VAR-NET nastavuje a komunikuje s ústřednou. Cena okruhu 5.000,- Kč bez DPH.
- Mapové rozhraní je nadstavbový grafický modul, pomocí něhož lze ovládat celou budovu. Kliknutím na vybraný prvek v mapě můžeme ovládat například otevření

a uzavření dveří, odtřežit či zastřežit zónu, kliknutím na kameru můžeme získat obraz z dané kamery. Graficky je také znázorněno, ve které zóně došlo k poplachu atd. Pomocí grafického rozhraní lze i monitorovat stav technologií. Cena mapového rozhraní je 25.000,- Kč bez DPH.



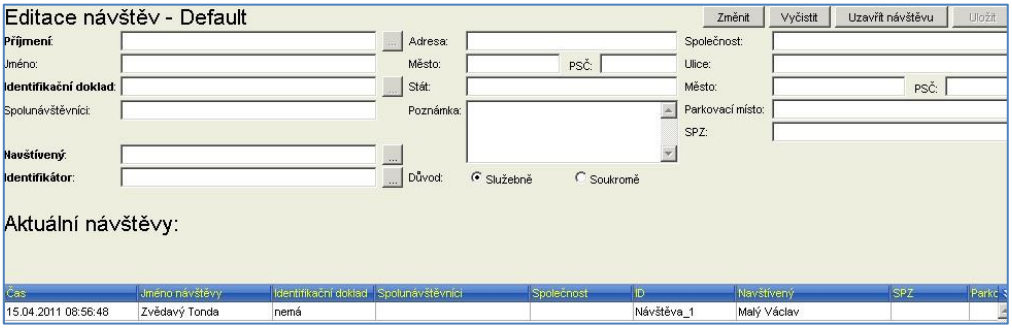
Obrázek 29: Mapové rozhraní Var-Net Integral [18]

- CCTV obsahuje v základu licenci na 8 kamer. Na každých dalších 8 kamer je nutno přikupovat další licence. Náhled uživatelského rozhraní na obr č. 30. Cena jednoho okruhu je 5.000,- Kč bez DPH.



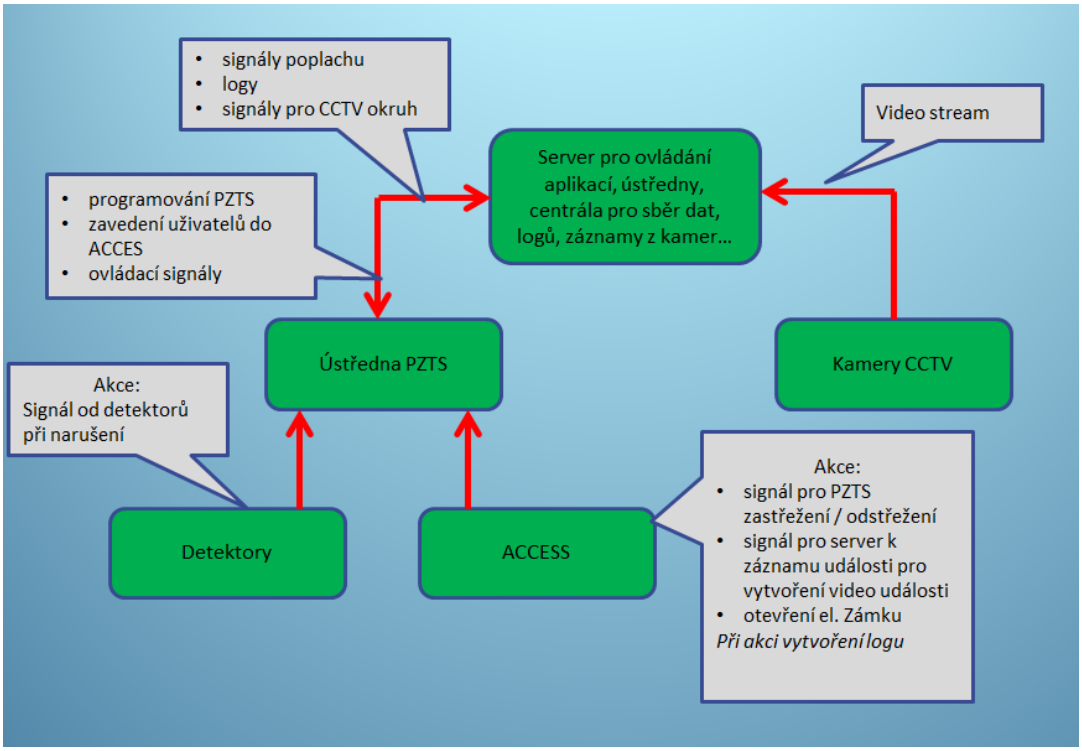
Obrázek 30: Náhled uživatelského rozhraní okruhu CCTV. [18]

- ACCESS je komunikační okruh přístup/docházka. V případě, že je ACCESS integrován do ústředny PZTS, není potřeba dokupovat licenci k tomuto modulu a nakupuje se pouze licence dle počtu osob s přístupem. Cena licence pro přístup 100 osob je 3.000,- Kč bez DPH.
- Recepce je okruh, jehož pořízením získáme sw nadstavbu pro zápis a evidenci návštěv v budově. Obrázek č. 31. Cena licence je 3.500,- Kč bez DPH.



Obrázek 31: Náhled uživatelského rozhraní modulu recepce. [18]

Blokové schéma signálů a funkcí systému je zobrazeno na obrázku č. 29. Z blokového schéma je patrné, že modul ACESS ovlivňuje akci zastřežení a odstřežení zón a dává prostřednictvím ústředny PZTS signál serveru pro vytvoření video události a záznamu logu. Dále detektory dávají signál ústředně o narušení. Prostřednictvím serveru lze přistupovat k ústředně, ovládat ji a programovat. Do serveru jsou přiváděny také poplachové signály a video stream z bezpečnostních IP kamer.



Obrázek 32: Blokové schéma signálů a obecných funkcí integrovaného systému.

7.4 Zabezpečení zabezpečených oblastí „V“ a „D“

V objektu budou dvě místnosti, které budou provozovány v režimu „Vyhrazené“ a „Důvěrné“. V místnosti kategorie Vyhrazené se bude nacházet IS Vydra pro zpracování vyhrazených informací a úschovný objekt kategorie Vyhrazené. Ve druhé zabezpečené místnosti bude zabezpečená oblast kategorie Důvěrné, ve které bude IS Dudek pro zpracování důvěrných informaci, s možností jejich uložení do úschovného objektu stejné kategorie. Tyto dvě zabezpečené místnosti budou vedle sebe. Při návrhu zabezpečení se musí vycházet ze stanovené míry rizika a požadovaného minimálního bodového ohodnocení, které je uvedeno v příloze č.1 vyhlášky č. 528/2005Sb.

7.4.1 Vyhodnocení hrozeb a stanovení míry rizika

V následujících odstavcích uvedu nejčastější rizika, provedu jejich okomentování a nakonec provedu jejich ohodnocení a stanovím míru rizika dle přílohy č.1 vyhlášky č. 528/2005Sb. a to ve třech stupních ***malé, střední, velké*** riziko.

a) *Hrozba neoprávněného nakládání s utajovanou informací oprávněnými osobami.*
V tomto případě může dojít k vyzrazení utajované informace jak z nedbalosti, tak z úmyslu. Mezi nedbalostní případy špatné manipulace s utajovanou informací patří

například zapomenutí utajovaného dokumentu oprávněným pracovníkem na stole apod. Dalším příkladem může být případ, kdy osobě skončí platnost pověření a opomene se této osobě zamezit přístup k utajovaným informacím. Správně musí být zamezen přístup do zabezpečených oblastí, zrušeny uživatelské účty v utajovaných informačních systémech atd.

Co se týče úmyslného vyzrazení, tak oprávněný pracovník může informace vynášet za úplatu nebo může být vydírán a podobně.

Míra rizika – STŘEDNÍ

b) *Hrozba neoprávněného nakládání s utajovanou informací neoprávněnými osobami*.

V tomto případě je přístup neoprávněných osob k utajovaným informacím zcela vyloučen, pokud budou dodrženy organizační pravidla uvedena v projektu fyzické bezpečnosti. Zde může pochybit oprávněný pracovník, který neoprávněnou osobu s utajovanou informací chtěně či nechtěně seznámí. Dalším rizikem může být vstup do zabezpečených oblastí násilným vloupáním nebo lstí.

Míra rizika – MALÁ

c) Hrozba poškození utajované informace průmyslovou havárií.

U této hrozby připadá u našeho objektu do úvahy například průmyslová havárie v sousedním objektu pro výrobu mléčných výrobků nebo výbuch plynu v kotelně, která obstarává centrální vytápění atd.

Míra rizika – STŘEDNÍ

d) Hrozba teroristického útoku.

Pokud jde o vyzrazení utajovaných informací za pomocí teroristického útoku, tak by se v tomto případě dalo stanovit riziko bezpochyby nízké, protože na budovy policie nebyly prováděny žádné teroristické útoky. Vzhledem k tomu, že v současné době je mezinárodní terorizmus na vzestupu, tak bych toto riziko z preventivních důvodů označil riziko střední.

Míra rizika – STŘEDNÍ

e) Hrozba vyzrazení utajované informace pasivním odposlechem.

Zde hrozí, že budou informace odposlouchávány přes okno a to buď odezíráním ze rtů nebo pozorováním obrazovky počítače. Dále může být odposlech pořizován z nízkofrekvenčních vibrací přenášených do rozvodů centrálního vytápění, ale také i z okenních výplní. Tyto přenášené vibrace odpovídají frekvenčním kmitočtům hovořících osob. Odposlech může být také pořízen záchytem frekvence, kterou

vyzařuje monitor a tímto odposlechem lze zjistit, co je na monitoru zobrazováno. Vzhledem k tomu, že budou předmětem ochrany pouze utajované informace stupně důvěrné a vyhrazené, stanovím míru rizika odposlouchávání těchto informaci na malou.

Míra rizika – MALÁ

Na základě vyhodnocení výše jmenovaných hrozeb stanovuji celkovou míru rizika jako **STŘEDNÍ.**

7.4.2 Návrh prostředků pro zabezpečení oblastí a bodové hodnocení povinných a nepovinných prvků

Nejprve se pro dané zabezpečené oblasti musí navrhnout certifikované prostředky k ochraně utajovaných informací. Seznam certifikovaných prostředků pro tyto účely nalezneme na webových stránkách NBÚ www.nbu.cz. Dle přílohy č. 1 vyhlášky č. 528/2005Sb jsou pro oblast kategorie Důvěrné povinné položky S1-S5 (S6 nepovinné), které se hodnotí bodově a součtem všech bodů pak získáme celkové ohodnocení zabezpečené oblastí. Jedná se o tyto položky:

- S1 – Celkové hodnocení úschovného objektu a jeho zámku
- S2 – Celkové hodnocení zabezpečené oblasti a jejího uzamykacího systému
- S3 – Hodnocení objektu
- S4 – Celkové hodnocení kontroly vstupu
- S5 – Celkové hodnocení ostrahy
- S6 – Celkové hodnocení ochrany perimetru - nepovinná položka

S1 - Návrh úschovného objektu

Jako úschovný objekt navrhuji trezor od firmy T - SAFE s.r.o., typ ASJ 3 (obrázek č. 32). Trezor má certifikát NBÚ ve stupni Důvěrné nebo Tajné. Rozvorový mechanismus je v uzamčeném stavu zajištěn klíčovým trezorovým zámkem. Rozměry V, Š, H, - 160, 60, 50 cm, hmotnost 220 kg, cena 25.660,- Kč bez DPH.

Tabulka 14: Bodové hodnoty trezoru ASJ 3 a číslo certifikátu NBÚ. [7]

Číslo certifikátu	Technic-ký pro-středek	Označení	Výrobce jméno	Držitel jméno	Kategorie použití	Počet bodů pro BS	Doba platnosti
T0054/2010	Skříňový trezor	typ ASJ 1 až ASJ 8, ASV 1, ASV 2, TZ 6/0, TZ 10/0	T - SAFE s.r.o.	T - SAFE s.r.o.	3	SS1=3, SS2=2	20.5.2013

Obrázek 33: Trezor od firmy T - SAFE s.r.o., typ ASJ 3. [16]

Získané body – SS1= 3, SS2 = 2.

S2 – Návrh zabezpečené oblasti a uzamykacího systému

Položka S2 se skládá z položky SS3, tj. hodnocení zabezpečené oblasti a SS4, hodnocení uzamykacího systému zabezpečené oblasti. Jak je výše uvedeno ve stavebně technickém popisu budovy, tak zabezpečená oblast vyhovuje požadavkům uvedených v příloze č. 1 vyhlášky č. 528/2005 Sb. pro typ zabezpečené oblasti 1. K dosažení bodového ohodnocení 2 schází lepší dveře a okna. Jedná se o obyčejné kancelářské dveře a obyčejná plastová okna bez certifikace RC2 dle ČSN EN 1627. Hranice zabezpečených oblastí jsou uvedeny v grafické příloze pod označením P3.

Protože lze předpokládat, že celkové bodové hodnocení bude vysoké, ponechám okna a dveře v současném stavu a uděluji zabezpečené oblasti SS3 1bod.

Jako uzamykací systém navrhuji cylindrickou vložku FAB 3000 Hd (tabulka č.15), která je certifikována NBÚ a určena pro kategorii 3 a bodové hodnocení dosahuje SS4 = 3. Cena této vložky je asi 1000,- Kč bez DPH.

Tabulka 15: Cylindrická vložka FAB 3000Hd a číslo certifikátu NBÚ. [7]

Číslo certifikátu	Technický prostředek	Označení	Výrobce jméno	Držitel jméno	Kategorie použití	Počet bodů pro BS	Doba platnosti
T0031/2011	Cylindrická vložka	FAB 3000 Hd	ASSA ABLOY Rychnov, s.r.o.	ASSA ABLOY Rychnov, s.r.o.	3	SS4=3	31.3.2013

Získané body – SS3 = 1, SS4 = 3.

S3 – Hranice objektu

V našem případě se jedná o objekt, který svými vlastnostmi splňuje bodové hodnocení objektu typu 3 (podmínky v příloze č. 1 vyhlášky č. 528/2005Sb.). Průlezné otvory ve výšce nad 5,5 m nemusí být zabezpečeny, v našem případě jsou ve výšce 8,25 m. Hranice objektu jsou vyobrazeny v grafické příloze pod označením P2.

Získané body – S3 = 3.

S4 – Celkové hodnocení kontroly vstupu

SS6 - Na všech vstupech do budovy je prováděna elektronická kontrola vstupu na základě identifikačního prvku, karty zaměstnance. Do zabezpečených oblastí se osoba dostane zadáním osobního PINu. Hodnota SS6 tedy dosahuje 1 bodu.

SS7 – Veškeré návštěvy mají doprovod oprávněné osoby, kterou je zaměstnance policie. Dále je vedena evidence o návštěvách. Z tohoto důvodu řešený objekt dostává bodové ohodnocení SS7 = 3 body.

Získané body – SS6 = 1, SS7 = 3

S5 – Celkové hodnocení ostrahy

SS8 – Ostrahu budou provádět 1 policista z pracoviště dozorčí služby, proto bude ostraha typu 2 s bodovým ohodnocením SS8=2.

SS91 – Zařízení elektrické zabezpečovací signalizace, které je pro objekt navrženo a v předchozí kapitole popsáno a splňuje požadavky typu 3, kdy zařízení je určeno pro střední až vysoké riziko dle normy ČSN EN 50131-1 a získává bodovou hodnotu SS91 = 3.

SS92 - Zařízení elektrické zabezpečovací signalizace je realizováno v zabezpečené oblasti v rozsahu prostorové a plášťové ochrany, kde jsou instalovány pohybové detektory a akustické detektory rozbití skla. Bodové hodnocení v tomto případě dosahuje SS92 = 2.

Získané body – SS8 = 2, SS91 = 3, SS92 = 2

S6 – Hodnocení ochrany perimetru – *nepovinná položka*

SS10 – bariéru zde tvoří zeď o výšce 2 m, což umožňuje získat 1 bod
SS11 – kontrola vstupu ve všech přístupových bodech perimetru – 1 bod
SS12 – nejsou prováděny žádné namátkové kontroly – 0 bodů
SS13 – není zde přítomen perimetrický detekční systém – 0 bodů
SS14 – je realizováno bezpečnostní osvětlení perimetru – 2 body

SS15 - v objektu je realizován televizní systém – 2 body

Finanční náklady na zřízení zabezpečených oblastí

Pokud bereme v potaz pouze vybavení zabezpečených oblastí, tak je potřeba pořídit 2 trezory. Trezory jsem navrhl od firmy T - SAFE s.r.o., typ ASJ 3 s cenou 25.660,- Kč bez DPH za kus. Pro vchodové dveře jsem navrhl cylindrickou vložku FAB 3000HD s cenou okolo 1.000,- Kč bez DPH za kus. Celkové náklady na pořízení vybavení pro dvě zabezpečené oblasti (kategorie Důvěrné a Vyhrazené) jsou 53.320,- Kč bez DPH**, s DPH 63.984,- Kč.**

7.4.3 Výpočet bodových hodnot

V následující části se budu věnovat výpočtu bodových hodnot pro kategorii Důvěrné. Této kategorii je podřazena kategorie Vyhrazené, a proto není potřeba provádět výpočet pro tuto kategorii za předpokladu, že i zabezpečená oblast V bude stejně chráněna jako zabezpečená oblast D. Bodové požadavky pro zabezpečenou oblast kategorie Důvěrné jsou uvedeny v tabulce č. 16. Dle vyhodnocených rizik a stanovení jejich míry jako střední, musí dané zabezpečené oblasti dosahovat minimálního bodového ohodnocení 14.

Tabulka 16: Bodové hodnoty pro zabezpečenou oblast kategorie Důvěrné. [2]

ZABEZPEČENÁ OBLAST KATEGORIE Důvěrné	**Míra rizika**		
	malá	střední	velká
Povinné : (S1) + (S2) + (S3)	6	8	9
Povinné : (S4) + (S5)	2	3	3
Nepovinné : (S6)	3	3	4
Celkový výsledek	**11**	**14**	**16**

Zabezpečené oblasti budou zařazeny do Třídy II, kdy vstupem do těchto oblasti nedochází k přímému seznámení s utajovanou informací.

Při výpočtu bodových hodnot budu využívat výborného pomocníka, program Výpočet bodového ohodnocení bezpečnostních opatření, verzi 2012 8.3. (obrázek č. 33), který naprogramoval Ing. Jiří Vařecha, pracovník bezpečnostního odboru Ministerstva vnitra. V aplikaci se navolí podmínky pro jakou kategorii je potřeba spočítat bodové ohodnocení a program automaticky vyhodnotí, které hodnoty S a SS jsou povinné či nepovinné tak, že povinné hodnoty znázorní podtržením. Po zadání hodnot klikneme na tlačítko výpočet a program vše spočítá a vyhodnotí. Vzorce pro výpočet celkového bodového hodnocení jsou uvedeny v příloze č. 1 vyhlášky č. 528/2005 Sb.

Obrázek 34: Program pro výpočet bodových ohodnocení zabezpečených oblastí. [21]

Po zadání výše zmíněných bodů S a dílčích bodů SS do programu bylo dosaženo následujícího celkového bodového ohodnocení:

Obrázek 35: Výsledek výpočtu bodového ohodnocení zabezpečených oblastí [21]

Závěrečné zhodnocení výpočtů

Cílem bylo dosažení celkového bodového ohodnocení minimálně 14-ti bodů. Toto bodové ohodnocení odpovídá minimu pro zabezpečenou oblast kategorie Důvěrné pro střední míru rizika. Navrhovaná technika, budova a organizační opatření dosahují celkového bodového ohodnocení pro povinné body S1-S5 21 bodů a pro nepovinné S6 bylo získáno 4 bodů. To znamená, že celkově bylo dosaženo 25 bodů a navrhované prostředky a opatření splňují předepsané požadavky pro ochranu utajovaných informací stupně Důvěrné (tabulka č. 16).

7.5 Orientační cenová kalkulace navrhovaného řešení

V následujících tabulkách jsou uvedeny HW a SW komponenty potřebné k realizaci projektu včetně výpočtů celkové ceny.

Tabulka 17: Cenová kalkulace PZTS a ACCESS technologie.

PZTS + ACCESS			
Název komponenty	**cena za 1ks bez DPH v Kč**	**počet ks**	**cena celkem bez DPH v Kč**
Ústředna Paradox Digiplex EVO 192 + BOX VT	5500	1	5500
Klávesnice Paradox K641	2600	3	7800
Detektor pohybu DM60 BUS detektor QUAD	800	46	36800
Detektor pohybu DOUBLE-TEC PIR+MW, AM	1000	13	13000
Akustický detektor rozbití skla DG457 GLASSTREK	700	20	14000
Akustický detektor Honeywell FG1625TAS	750	2	1500
Signalizace vnitřní - SA913	230	1	230
Signalizace venkovní BELL-TEC SIREN	430	1	430
ACCESSPACK 910-ACM12+R910	4700	19	89300
Elektromechanický zámek dveří 17RR-E4	1200	19	22800
Kabeláž VL 06-6x0,22 (100m)	750	4	3000
celkem			**194360**

Tabulka 18: Cenová kalkulace CCTV systému.

CCTV			
Název komponentu	**cena za 1ks bez DPH v Kč**	**počet ks**	**cena celkem bez DPH v Kč**
ACTi TCM-7411 (antivandal)	11400	3	34200
ACTi TCM-1231 (statická)	12200	7	85400
ACTi CAM-6630P (PTZ)	52000	2	104000
celkem			**223600**

Tabulka 19: Cenová kalkulace integračního HW a SW řešení.

Integrační HW a SW řešení			
Název komponentu	**cena za 1ks bez DPH v Kč**	**počet ks**	**cena celkem bez DPH v Kč**
DELL PowerEdge T110 II	25000	1	25000
DGP LAN V +	3400	1	3400
switch Micronet 24/24+2 MN	12800	1	12800
Windows Web Server 2008	6000	1	6000
INTEGRAL - jádro	5000	1	5000
INTEGRAL - okruh PZTS	5000	1	5000
INTEGRAL - okruh CCTV	5000	2	10000
INTEGRAL - návštěvy	3500	1	3500
INTEGRAL - přístup 100 osob	3000	2	6000
INTEGRAL - mapové rozhraní	25000	1	25000
celkem			**101700**

Jak vyplývá z výše uvedených cenových tabulek, tak by celková cena za materiál a software měla být 519.660,- Kč bez DPH. Cena včetně DPH by pak byla 623.592,- Kč. Cena instalace se pohybuje přibližně 0,7 ceny hardwaru. Cena instalačních prací pak bude 436.514,- Kč s DPH.

Cena za technické zabezpečení: hardware, software a instalační práce by pak mohla být **1.060.106,- Kč s DPH.**

Náklady na vybavení zabezpečených oblastí kategorie Vyhrazené a Důvěrné tvoří **63.984,- Kč s DPH.**

Celkový finanční rozpočet na pořízení technického zabezpečení budovy a prostředků pro ochranu utajovaných informací by dle propočtů mohl být přibližně ve výši **1.124.090,- Kč s DPH.**

8. NOVÉ ORGANIZAČNÍ SCHÉMA A BEZPEČNOSTNÍ DOPORUČENÍ

V této kapitole se pokusím navrhnout provozní řád - organizační schéma, které by odpovídalo danému objektu. Pokusím se podchytit ty nejdůležitější oblasti mající významný vliv na bezpečnost budovy a vlastně celého areálu.

V areálu bude prováděn základní režim bezpečnostní ochrany. Tutu ochranu bude tvořit:

- **Fyzická ostraha areálu**, která bude zabezpečena pracovníky ostrahy (policisté sloužící dozorčí službu)
- **Režimová opatření**, která určí pravidla pro vstup, výstup a vjezd do objektu. Dále budou určena pravidla pro pohyb osob v areálu a v jeho částech. Součástí bude i systém klíčového hospodářství.
- **Technické prostředky**, které ztíží vstup do areálu a zabezpečených oblastí nebo vyvolají poplach ve střežených zónách.

Vstup a vjezd do areálu

Vstup do areálu bude možný pouze pomocí hlavního vstupu přes recepci (západní strana areálu). Vstup na recepci bude otevřen pro veřejnost v pracovní dny od 07:00 do 18:00 hodin a v době od 18:00 do 07:00 bude vstup uzavřen a na recepci bude možný přístup pouze pro zaměstnance, kteří se autorizují vůči přístupovému bodu do recepce. V ostatní dny jako víkendy, svátky a podobně bude po celou dobu vstup na recepci uzavřen. Dveře vedoucí z recepce dále do areálu jsou opatřeny kontrolou vstupu a každý zaměstnanec se bude muset autorizovat na čtečce karet pomocí služební karty a po autorizaci mu bude umožněn další přístup do budovy. Podrobněji a přehledně je řešen přístup do budovy včetně časových zón v tabulce č. 20. V tabulce č. 21 je zobrazena bezpečnostní politika pohybu osob po objektu. Objekt jsem rozdělil na 15 bezpečnostních zón. Vyobrazení zón je pak řešeno ve výkresech, které jsou přílohou diplomové práce.

Vjezd do areálu bude možný pouze přes vjezd do dvora, který bude opatřen rolovací bránou. Samostatný průchod přes vjezdovou bránu bude zakázán. Tento vjezd bude sloužit pouze vozidlům Policie ČR a MV. Na tomto vjezdu bude kontrola vstupu, proto se bude muset každý zaměstnance autorizovat na čtečce svoji služební kartou. Zaměstnanec po průjezdu branou bude moci pokračovat v jízdě až po úplném uzavření brány, aby se zabránilo neoprávněnému vstupu do areálu.

Oba dva přístupy do budovy ze dvora jsou opatřeny kontrolou vstupu se čtečkou karet. Každý zaměstnance se musí vůči této čtečce autorizovat.

Osoby oprávněné k samostatnému vstupu do areálu nesmí umožnit vstup jiné neoprávněné osobě s výjimkou doprovázených návštěv.

Tabulka 20: Politika práv přístupu do budovy v závisloti na čase a příslušnosti ke skupině uživatelů budovy

Skupina	Pracovní den (07-18 hodin)	Pracovní den (18-07 hodin)	víkend (celý den)	státní svátek (celý den)
Dozorčí	A	A	A	A
Policisté OOP	A	A	A	A
Policisté SKPV	A	A	A	A
Určení policisté	A	A	A	A
Vedoucí pracovníci	A	A	A	A
Sekretariát	A	A	A	A
Policisté ostatních útvarů	A	-	-	-
Recepční	A	-	-	-
IT Technici	A	A	A	A
Údržba	A	A	A	A
Uklizečky	A	-	-	-
Návštěvy	A	-	-	-

Legenda: A = umožněn přístup

Tabulka 21: Politika práv pohybu osob po budově

Skupina	Zóna 1	Zóna 2	Zóna 3	Zóna 4	Zóna 5	Zóna 6	Zóna 7	Zóna 8	Zóna 9	Zóna 10	Zóna 11	Zóna 12	Zóna 13	Zóna 14	Zóna 15
Dozorčí	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
Policisté OOP	-	-	-	-	-	-	A	A	A	A	-	-	-	-	A
Policisté SKPV	-	-	-	-	-	-	-	A	A	A	-	A	-	-	A
Určení policisté	-	-	-	-	A	A	A	A	A	A	-	-	-	-	A
Vedoucí pracovníci	A	-	-	-	-	-	A	A	A	A	-	A	-	A	A
Sekretariát	-	-	-	-	-	-	-	A	A	A	-	-	-	A	A
Policisté ostatních útvarů	-	-	-	-	-	-	-	A	A	A	-	-	-	-	A
Recepční	-	-	-	-	-	-	A	A	A	A	-	-	-	-	A
IT Technici	-	-	-	-	-	-	A	A	A	A	-	A	A	A	A
Údržba	-	-	-	-	-	-	A	A	A	A	A	A	-	A	A
Uklízečky	-	-	-	-	-	-	A	A	A	A	-	A	-	A	A
Návštěvy	-	-	-	-	-	-	-	-	-	A	-	-	-	-	-

Legenda: A = umožněn přístup

Tabulka 22: Popis jednotlivých zabezpečených zón

Zóna	místo v budově
Zóna 1	Místnost pro výkon dozorčí služby
Zóna 2	Sklad zbraní
Zóna 3	Chodba k policejním celám
Zóna 4	Policejní cely
Zóna 5	Zabezpečená oblast - Vyhrazené
Zóna 6	Zabezpečená oblast - Důvěrné
Zóna 7	Oddělení OOP
Zóna 8	Hala v 1. NP
Zóna 9	Chodba k recepci
Zóna 10	Recepce
Zóna 11	Oddělení SKPV
Zóna 12	Technická místnost
Zóna 13	Serverovna
Zóna 14	Vedení
Zóna 15	Přednáškový sál, hala

Pohyb návštěv v areálu

Návštěvy budou moci samostatně vstupovat do prostorů recepce ve stanovené době. Vstupovat a pohybovat se v ostatních částech areálu bude možný pouze za doprovodu oprávněné osoby. Oprávněná osoba bude povinna návštěvu doprovázet po celou dobu trvání návštěvy a zajistit, aby ze strany návštěvy nedošlo k ohrožení předmětů chráněného zájmu, případně škodě na majetku. Návštěva se bude muset při vstupu na recepci prokázat zaměstnanci recepce dokladem totožnosti a sdělit účel návštěvy. Recepční provede zápis do evidence návštěv a vyrozumí navštěvovanou osobu, aby si pro návštěvu na recepci přišla. Na výzvu se navštěvovaná osoba bude muset podrobit vstupní kontrole, včetně zavazadel apod., pomocí detekční techniky. Po skončení návštěvy pak provede zaměstnanec recepce záznam do evidence návštěv.

Pravidla pro manipulaci s klíči

Klíče od všech vstupních dveří do budovy budou uloženy v místnosti pro výkon dozorčí služby, která bude i vykonávat ostrahu objektu. Klíče od samostatných kanceláří, kde zaměstnanec pracuje, bude mít tyto klíče u sebe a zodpovídat za ně. Všechny přidělené klíče budou evidovány v knize evidence klíčů případně v příslušné SW aplikaci. Všechny záložní klíče budou uloženy v uzamykatelné skříni u dozorčí služby. Pokud někdo bude

chtít vydat záložní klíč, provede záznam o tom, jaký klíč a komu ho vydává. Pokud bude žadatel chtít záložní klíč od místnosti, ke které nemá přiřazen klíč, dozorčí vyrozumí vedoucího daného oddělení a po domluvě tento klíč vydá a provede o tom záznam.

U zabezpečených oblastí a úschovných objektů jsou klíče uloženy ve speciální uzamykatelné skříňce u dozorčí služby. Žadatel o tyto klíče se musí nahlásit dozorčímu, který provede kontrolu, zda je žadatel vedený jako oprávněná osoba. O vydání provede záznam do příslušné evidence a uvede, komu klíče vydal, čas převzetí a čas odevzdání.

Všechny klíče u dozorčí služby musí být označeny štítkem s identifikací místností, ke kterým jsou klíče určeny (číslo místnosti), popřípadě musí být uvedeno, zda se jedná o zabezpečenou oblast úschovný objekt apod.

Duplikáty klíčů od vstupů do objektu, zabezpečených oblastí a úschovných objektů budou pořizovány jen v odůvodněných případech na pokyn vedoucího areálu. Jinak pří ztrátě těchto klíčů musí být podniknuty takové kroky, aby nedošlo k ohrožení předmětů chráněného zájmu, případně škodě na majetku.

Ochrana předmětu chráněného zájmu v režimových prostorech

Režimovými prostory se rozumí zejména policejní cely, sklady zajištěných věcí pocházející z trestné činnosti, zbrojní sklady, zabezpečené oblasti a další určené prostory. Do režimových prostor budou moci vstoupit a samostatně se v nich pohybovat pouze jejich uživatelé nebo osoby odpovědné za jejich chod. Ostatní osoby mohou do režimových prostor vstupovat pouze s doprovodem oprávněné osoby. Režimové prostory budou v době nepřítomnosti oprávněné osoby řádně uzavřeny, bude aktivován PZTS. Vstupní dveře do režimových prostor V a D musí být pečetěny oprávněnou osobou. Dveře musí být opatřeny štítkem se seznamem, na kterém budou uvedeny oprávněné osoby a jejich čísla pečetí.

Ochrana utajovaných informací

Ochrana utajovaných informací a pravidla pro zpracování, manipulaci a ukládání utajovaných informací jsou vždy řešena v daném projektu fyzické bezpečnosti objektu.

Technické prostředky

K ochraně areálu jsou využity elektrotechnické a mechanické prostředky. Elektrotechnická ochrana je zabezpečována systémem PZTS, přístupovým systémem a kamerovým systémem. Tyto systémy jsou navzájem integrovány do kompaktního celku.

Ostraha areálu

Ostraha objektu bude prováděna policisty sloužící dozorčí službu. Ostraha bude ke střežení využívat kamerový systém a bude obsluhovat poplachové příjímací centrum. Ostraha areálu bude provádět výkon služby ve 12-ti hodinových pracovních směnách. Policisté dozorčí služby budou provádět 2 x za svoji službu v náhodně zvolených časech obchůzku areálu. Dozorčí služba odpovídá za ostrahu areálu, ostrahu zabezpečených oblastí, režim policejních cel a klíčové hospodářství. Výkon dozorčího bude za normální situace vykonávat jeden policista.

Bezpečnostní opatření proti mimořádným událostem

Do areálu bude zakázáno vstupovat se zbraní s výjimkou příslušníků Policie a jiných ozbrojených bezpečnostních sborů. Dále bude zakázáno do areálu vstupovat s nebezpečnými předměty, které by mohly ohrozit bezpečnost osob nebo způsobit škodu na majetku a technickém vybavení.

DÍLČÍ ZÁVĚR PRAKTICKÉ ČÁSTI

Praktická část byla rozdělena do čtyř samostatných kapitol. V první kapitole praktické části jsem provedl analýzu současného stavu ochrany budovy policie včetně stavebně technického popisu. Druhou kapitolu jsem věnoval návrhu požadavků pro systém PZTS, ACCESS a CCTV. V následující části obeznamuji čtenáře s návrhem integrovaného technického zabezpečení budovy. Systém PZTS jsem navrhl vybudovat na ústředně Digiplex EVO 192. Pro výstavbu ACCESS systému jsem navrhl využít nadstavbové ACCESS moduly pro ústřednu Digiplex EVO 192, které se k ní připojují po sběrnici. Systém CCTV jsem se rozhodl postavit výhradně na IP technologii, kdy se o záznam obrazu bude starat integrační server se softwarem VAR-NET INTEGRAL. Dále jsem v diplomové práci navrhl potřebné vybavení pro zabezpečené oblasti a výpočtem celkového bodového ohodnocení jsem si ověřil, zda bude navrhované řešení splňovat legislativní podmínky z hlediska OUI. Orientační cenu jsem vyčíslil včetně montáže, kabeláže, komponent, SW a prostředků pro ochranu utajovaných informací na 1.124.090,- Kč s DPH. V poslední kapitole praktické části jsem provedl návrh nového organizačního schématu.

ZÁVĚR

Cílem této diplomové práce byl návrh nového zabezpečení pro budovu Policie ČR v souladu se stanovenými body zadání. První díl diplomové práce tvoří část teoretická, kterou jsem rozdělil do čtyř okruhů tak, aby v nich bylo zahrnuto vše podstatné k řešené problematice a čtenář získal základní přehled z daných oblastí, které jsou klíčové k řešení stanoveného problému. Druhý díl diplomové práce, praktická část, je tvořena analýzou s následným návrhem bezpečnostního řešení objektu.

V první kapitole teoretické části jsem rozebral význam a související pojmy s problematikou ochrany utajovaných informací a uvedl jsem potřebné legislativní normy. Podstatná část je také věnována fyzické bezpečnosti z hlediska OUI, ale také například roli Národního Bezpečnostního Úřadu. Zpracování této problematiky bylo v této práci nevyhnutelné z toho důvodu, že v objektu policie se bude nacházet zabezpečená oblast kategorie Vyhrazené a Důvěrné a bylo tedy nutné respektovat i legislativu s tímto spojenou. V další části teorie jsem se zaměřil na technickou a mechanickou ochranu objektů. Vzhledem k tomu, že se jedná o poměrně široké téma, zaměřil jsem se především na důležité části, které se budou dotýkat řešení daného problému. Cílem tedy není čtenáře seznámit se všemi možnými detektory, komponenty a způsoby ochrany, ale především se v této části dotknout toho, co by mohlo být k řešení problému využíváno v praktické části diplomové práce. Protože jsem měl vizi, že by dané řešení mohlo být založeno i na integraci bezpečnostních aplikací, věnoval jsem celou třetí část diplomové práce této problematice tak, abych čtenáře seznámil se základním rozdělením, principy a druhy integrace. V poslední části teorie jsem zmínil potřebnou legislativu a technické normy, které se dotýkají řešeného problému.

Hned v prvním úseku praktické části je řešený objekt podroben analýze současného stavu zabezpečení. V této části jsem provedl analýzu stavebně technického stavu budovy včetně toho, jak je situována. Dále jsem provedl podrobné vyhodnocení perimetru, plášťové, prostorové a předmětové ochrany. V této části jsem také analyzoval současné organizační schéma daného objektu. Další kapitola diplomové práce řeší požadavky na nové zabezpečení objektu. Jsou zde zmíněny obecné požadavky na systém PZTS, kamerový a přístupový systém a to vše v takovém kontextu, aby byly dané systémy integrovány do jednoho funkčního celku. Z těchto požadavků na zabezpečení a analýzy současného stavu objektu vychází následně další kapitola, která se zabývá návrhem technického zabezpečení.

Hardware je navrhnut tak, aby bylo vše navzájem kompatibilní a funkční v rámci požadované integrace bezpečnostních aplikací. Jako integrační řešení jsem využil VAR-NET-INTEGRAL, řešení od firmy VARIANT plus s.r.o. S touto firmou jsem i řešení daného problému několikrát konzultoval. Systém VAR-NET-INTEGRAL umožňuje integrovat do jednoho funkčního celku požadované bezpečnostní aplikace, včetně nastavení jejich vzájemných vazeb. Systém bude hardwarově postaven na řešení od kanadské firmy Paradox. Celý PZTS je vybudován na sběrnicovém systému. Jako ústředna PZTS je použita ústředna Digiplex EVO 192. K této ústředně jsou po sběrnici připojeny potřebné detektory. Přístupový systém jsem vyřešil nadstavbovým modulem ústředny, který je dodáván včetně čteček. Tento modul je připojen k ústředně po sběrnici. V této části diplomové práce jsem navrhl i IP kamerový systém postavený na kamerách značky ACTi. Využil jsem právě tyto kamery, protože k nim má firma VARIANT vyvinuté drivery, které využívá server VAR-NET INTEGRAL a pomocí těchto driverů přistupuje ke kamerám. V této části diplomové práce jsem zmínil i potřebné integrační hardwarové prvky jako je například PoE switch pro IP kamery nebo převodník pro přenos dat z ústředny PZTS/LAN. Dále jsem zde provedl návrh prostředků pro vybavení zabezpečených oblastí tak, aby celkový bodový součet hodnot odpovídal legislativním požadavkům pro ochranu utajovaných informací. U komponent a prostředků, u kterých je to nutné z hlediska významu ochrany utajovaných informací, jsem přehledně uvedl tabulky, které obsahují číslo certifikátu NBÚ a jeho platnost včetně získaných bodových hodnot. S využitím těchto bodových hodnot byly prováděny i potřebné výpočty. V poslední části diplomové práce jsem navrhl nové organizační schéma provozu budovy. Organizační schéma řeší provoz objektu, vstup a vjezd do areálu, režim pohybu návštěv po objektu nebo také například ostrahu a klíčové hospodářství. Celkovou cenu bezpečnostního řešení jsem odhadl včetně montáže, kabeláže, komponent a prostředků pro ochranu utajovaných informací na 1.124.090,- Kč s DPH.

Přínos práce spatřuji především ve vyřešení aktuální bezpečnostní situace, která nastala v rámci organizačních změn. Současný stav ochrany budovy a jiných chráněných zájmů je velmi slabý, lehce zranitelný a bez aplikace ochrany utajovaných informací. V diplomové práci je navržen integrovaný bezpečnostní systém, který zvyšuje bezpečnost objektu a přináší mimo jiné i jeho komfortnější užívání. Je zde také proveden návrh na zřízení zabezpečených oblastí, které budou sloužit pro ochranu utajovaných informací a návrh organizačního schématu provozu. Tato práce by mohla být využita jako hotový projekt

řešící komplexní zabezpečení budovy nebo by mohla sloužit jako inspirace bezpečnostním pracovníkům zařazených na oddělení technické ochrany policii ČR. Tito pracovníci by pak měli k dispozici projekt, který by jim poskytnul náhled na jeden z možných způsobů řešení integrace, která prozatím není u policie ČR žádným způsobem aplikována.

Conclusion

The main aim of the diploma thesis has been focused on designing of the new building for the security police in accordance with the established entry points. The first part of the thesis has been consisted of a theoretical part, which is divided into four areas, so there has been included everything essential to solving the problems. The reader gets an overview of the areas in question, which are the key to solving the problem.

In the first chapter there I have analyzed the meaning and concepts related to the issue of protection of classified information using the legislative standards. A substantial portion is devoted to physical security in terms protection of classified information, but also for the role of the National Security Office. The treatment of this issue in this work was inevitable; there will be located areas like RESTRICTED and CONFIDENTIAL. That is absolutely necessary to respect the legislation associated with this. In another part of the theory there I have focused on technical and mechanical protection of objects. This is given in a fairly broad topic; I have focused mainly on the important parts that will affect the solution of the problem. The thesis should have to familiarize the reader with all kinds of detectors, components and methods of protection. I had a vision that the solution could be based on the integration of safety applications, so the third part of the thesis has solved the principles and types of integration. In the last part of the theory there I have mentioned the necessary legislation and technical standards that affect the problem being solved.

In the very first section of the practical part there has been analyzed the current situation of security. In this section, there I have analyzed the structural and technical condition of the building. I also have made a detailed evaluation of the perimeter, plastic, spatial and object protection. In this section there I have showed the current organizational chart of the object. Another chapter of the thesis included the requirements of the new security building. There are mentioned general requirements for I & HAS system, CCTV and access control system and all in such a context that the systems were integrated into a single functional unit. These security requirements and analysis of the current state of the object will be described in next chapter. The hardware has been designed in compatibility with desired integration of security applications. As an integration solution I have used VAR-NET-INTEGRAL, solutions from VARIANT plus Ltd. Company. I also addressed the problem several times and consulted with the company at all. The system VAR-NET-INTEGRAL has been integrated into one functional unit required security applications,

including setting their relationship. The system has to be built on a hardware solution from the Canadian company Paradox. The entire I & HAS is built on the bus system. As the panel I & HAS is using Digiplex EVO 192. This control panel is connected to the bus required detectors. The access system is designed by superstructure PBX module that comes with readers. This module is connected to the PBX via the bus. In this part of the thesis is designed IP address by CCTV system based on ACTi brand cameras. I used these cameras from VARIANT Company. In this part of the thesis there have been discussed necessary hardware integration features such as PoE switch for IP camera or converter for data transmission - I & HAS PBX / LAN. There have been also a proposal of funds for equipment security areas, so that the total sum of the point values corresponded to the legislative requirements for protecting classified information. For components and equipment, where it is necessary in terms of the importance of protecting classified information, there is a table consisted of NSO number certificate and its validity, including acquired point values. Using these point values were also carried out the necessary calculations. In the last part of the thesis I have proposed a new organizational chart of operation of the building. Organizational scheme solves operation of the building, the entrance and the entrance to the complex, the mode of movement of visitors around the premises or also, for example security and key management. Total indicative cost security solution has been figured including installation, wiring, components and equipment for the protection of classified information at 1.124.090,- CZK with VAT.

I have found the benefits of the diploma thesis in resolving the current security situation that could occurred in the organizational change. The current conservation status of buildings and other protected interests is very weak, vulnerable and easily without using the protection of classified information. The thesis has proposed an integrated security system that improves the security of the building and provides an inter alia, so it’s comfortable to use. It has also made a proposal to establish secure areas, which would serve for the protection of classified information and draft organizational chart of the operation. That work could be used as a finished project addressing complex security or could serve as an inspiration to security personnel assigned to the Department of Technical Protection Police. These workers could then have a project that would grant them insight into one of the possible solutions to integration. That has not been applied in the police system in any way yet.

Seznam použité literatury

[1] ČESKO. Zákon č. 412 ze dne 21. září 2005 o ochraně utajovaných informací a o bezpečnostní způsobilosti jak vyplývá z pozdějších změn. In: *Sbírka zákonů České republiky*. 2012, s. 1890-1958. částka 47, ISSN 1211-1244

[2] ČESKO. Vyhláška č. 528 ze dne 14.12.2005 o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb. In: Sbírka zákonů České republiky. 2011, částka 155, s. 5888-5916. ISSN 1211-1244

[3] MUSIL, Rudolf. *Ochrana utajovaných skutečností*. 1. vyd. Praha: Eurounion, 2001, 379 s. ISBN 80-858-5893-2.

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

[5] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management II.* 1. vyd. Zlín: VeRBuM, 2012, 386 s. ISBN 978-80-87500-19-4.

[6] VALOUCH, Jan. UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ. *Projektování integrovaných poplachových systémů: elektronická učební pomůcka*. 2012.

[7] *Národní bezpečnostní úřad* [online]. 2013 [cit. 2013-01-26]. Dostupné z: http://www.nbu.cz/

[8] NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD. *Certifikační postup NBÚ*. Praha, 2012.

[9] ČSN EN 50131. *Poplachové systémy: Poplachové zabezpečovací a tísňové systémy.* 2. vyd. Praha: Český normalizační institut, 2007.

[10] ACCES. *Elektronické zabezpečení objektů* [online]. 2005 [cit. 2013-01-28]. Dostupné z: http://www.acces.cz

[11] IVANKA, Ján. *Systemizace bezpečnostního průmyslu I*. Vyd. 3. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009, 123 s. ISBN 978-80-7318-850-4.

[12] ADÁMEK, Milan. UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ. *Úvod do studia předmětu Kamerové systémy: elektronická učební pomůcka*. 2012.

[13] ČESKO. Zákon č. 101 ze dne 4. dubna 2000 o ochraně osobních údajů In: *Sbírka zákonů České republiky*. 2000. částka 32

[14] ČSN CLC/TS 50398. *Poplachové systémy: Kombinované a integrované systémy*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví., 2009

[15] Conrad Electonic. *Conrad Electronic - obchod s elektronikou a technikou* [online]. [cit. 2013-02-27]. Dostupné z: http://www.conrad.cz/

[16] Trezor.cz. *Trezor.cz* [online]. 2013 [cit. 2013-02-28]. Dostupné z: http://www.trezor.cz/archivacni-trezory/archivacni-trezor-asj-3.html

[17] VARIANT PLUS, spol. s r.o. *Variant.cz* [online]. [cit. 2013-03-05]. Dostupné z: http://www.variant.cz/

[18] VARIANT PLUS, spol. s r.o. *integracebudov.cz* [online]. [cit. 2013-03-11]. Dostupné z: http://www.integracebudov.cz/

[19] Alfacomp.cz. *Alfacomp* [online]. [cit. 2013-03-11]. Dostupné z: http://www.alfacomp.cz

[20] Eshop-zabezpeceni.cz. *eshop-zabezpeceni.cz* [online]. [cit. 2013-03-11]. Dostupné z: http://www.eshop-zabezpeceni.cz

[21] VAŘECHA, Jiří. BEZPEČNOSTNÍ ODBOR MINISTERSTVA VNITRA. [cit. 2013-03-11]. *Výpočet bodového ohodnocení bezp. opatření verze 2012. 8. 3. 2012.*

Seznam použitých symbolů a zkratek

CCD	Charge coupled device – součástka používaná pro snímání obrazové informace
CCTV	Closed circuit television – Uzavřený televizní okruh
CMOS	Complementary Metal Oxide Semiconductor - součástka používaná pro snímání obrazové informace
ČSN	Česká státní norma
I&HAS	Intruder and Hold-up Alarm System – Poplachový zabezpečovací tísňový systém
LAN	Local Area Network – Místní počítačová síť
NBU	Národní bezpečnostní úřad
OUI	Ochrana utajovaných informací
PGM	ProGraMmable output – Programovatelný výstup ústředny PZTS
PIR	Passive Infrared Receiver – Pasivní infračervený detektor
PoE	Power over Ethernet – Nápájení zařízení prostřednictvím ethernetu
PPC	Poplachové příjímací centrum
PTZ	Pan Tilt Zoom – Vzdálená telemetrie
PZTS	Poplachový zabezpečovací tísňový systém
SIE	Systémová elektroinstalace

Seznam obrázků

Obrázek 1: Vzor certifikátu technického prostředku 21
Obrázek 2: Blokové schéma přístupového bodu. 27
Obrázek 3: Možnosti aplikace integrovaných systémů v komerčních objektech 34
Obrázek 4: Obecné schéma HW integrace IN/OUT 36
Obrázek 5: Obecné schéma HW integrace, PZTS jako ústředna modulárního systému 37
Obrázek 6: Obecné schéma HW integrace – automatizační systém jako integrační prvek 38
Obrázek 7: Konektor RJ 45, BNC a RJ11 38
Obrázek 8: Obecné schéma integrovaného poplachového systému propojení LAN/WAN 39
Obrázek 9: Obecné schéma aktivačních a reakčních vazeb v integrovaném systému 41
Obrázek 10: Situační plán řešeného objektu 46
Obrázek 11: PIR detektory používané k prostorové ochraně 48
Obrázek 12: Ústředna DSC typ PC2510CZ2. 48
Obrázek 13: Klávesnice DSC PC 2550RK. 49
Obrázek 14: Obousměrné komunikační zařízení od firmy Fides - FA101. 49
Obrázek 15: Ústředna Paradox EVO 192. 55
Obrázek 16: Klávesnice Paradox K641 57
Obrázek 17: Detektor pohybu DM60 BUS detektor QUAD 58
Obrázek 18: Detektor pohybu DOUBLE-TEC PIR+MW, AM. 59
Obrázek 19: Akustický detektor rozbití skla DG457 GLASSTREK 60
Obrázek 20: Signalizace vnitřní - SA913 61
Obrázek 21: Signalizace venkovní BELL-TEC SIREN 62
Obrázek 22: Proximity čtečka Paradox R910 s access modulem ACM12 63
Obrázek 23: Elektromechanický zámek 17RR-E4 64
Obrázek 24: IP kamera ACTi TCM-7411 65
Obrázek 25: IP kamera ACTi TCM-1231 65
Obrázek 26: IP kamera ACTi CAM-6630P 66
Obrázek 27: Blokové schéma zapojení ústředny do sítě LAN přes převodník 67
Obrázek 28: Obecná schéma hardwarové integrace bezpečnostních aplikací 68
Obrázek 30: Mapové rozhraní Var-Net Integral 70
Obrázek 31: Náhled uživatelského rozhraní okruhu CCTV 70

Obrázek 32: Náhled uživatelského rozhraní modulu recepce..... 71
Obrázek 29: Blokové schéma signálů a obecných funkcí integrovaného systému. 72
Obrázek 33: Trezor od firmy T - SAFE s.r.o., typ ASJ 3..... 75
Obrázek 34: Program pro výpočet bodových ohodnocení zabezpečených oblastí..... 78
Obrázek 35: Výsledek výpočtu bodového ohodnocení zabezpečených oblastí 78

Seznam tabulek

Tabulka 1: Bodové hodnoty nejnižší míry zabezpečení zabezpečené oblasti kategorie Přísně tajné 18
Tabulka 2: Bodové hodnoty nejnižší míry zabezpečení zabezpečené oblasti kategorie Vyhrazené 19
Tabulka 3: Legislativní a technické normy 42
Tabulka 4: Základní technické vlastnosti ústředny Paradox EVO 192 56
Tabulka 5: Informace o certifikátu uděleným NBÚ pro ústřednu Paradox EVO 192 57
Tabulka 6: Základní technické vlastnosti klávesnice K641 58
Tabulka 7: Základní technické vlastnosti pohybu DM60 BUS detektor QUAD 59
Tabulka 8: Technické parametry Detektor pohybu DOUBLE-TEC PIR+MW, AM 59
Tabulka 9: Informace o certifikátu detektoru pohybu DOUBLE-TEC PIR+MW, AM. 60
Tabulka 10: Informace o certifikátu detektoru rozbití skla Honeywell FG1625TAS 61
Tabulka 11: Technické parametry detektoru rozbití skla Honeywell FG1625TAS 61
Tabulka 12: Technické parametry čtečky karet Paradox R910 63
Tabulka 13: Technické parametry access modulu ACM12 63
Tabulka 14: Bodové hodnoty trezoru ASJ 3 a číslo certifikátu NBÚ 74
Tabulka 15: Cylindrická vložka FAB 3000Hd a číslo certifikátu NBÚ 75
Tabulka 16: Bodové hodnoty pro zabezpečenou oblast kategorie Důvěrné 77
Tabulka 17: Cenová kalkulace PZTS a ACCESS technologie. 79
Tabulka 18: Cenová kalkulace CCTV systému. 79
Tabulka 19: Cenová kalkulace integračního HW a SW řešení. 80
Tabulka 20: Politika práv přístupu do budovy v závisloti na čase a příslušnosti ke skupině uživatelů budovy 82
Tabulka 21: Politika práv pohybu osob po budově 82
Tabulka 22: Popis jednotlivých zabezpečených zón 83

Seznam Příloh

P 1 Situace řešeného objektu

P 2 Hranice zabezpečeného objektu z hlediska OUI

P 3 Hranice zabezpečených oblastí OUI – 1.NP

P 4 1NP severní křídlo budovy – zakreslení techniky

P 5 1NP západní křídlo budovy – zakreslení techniky

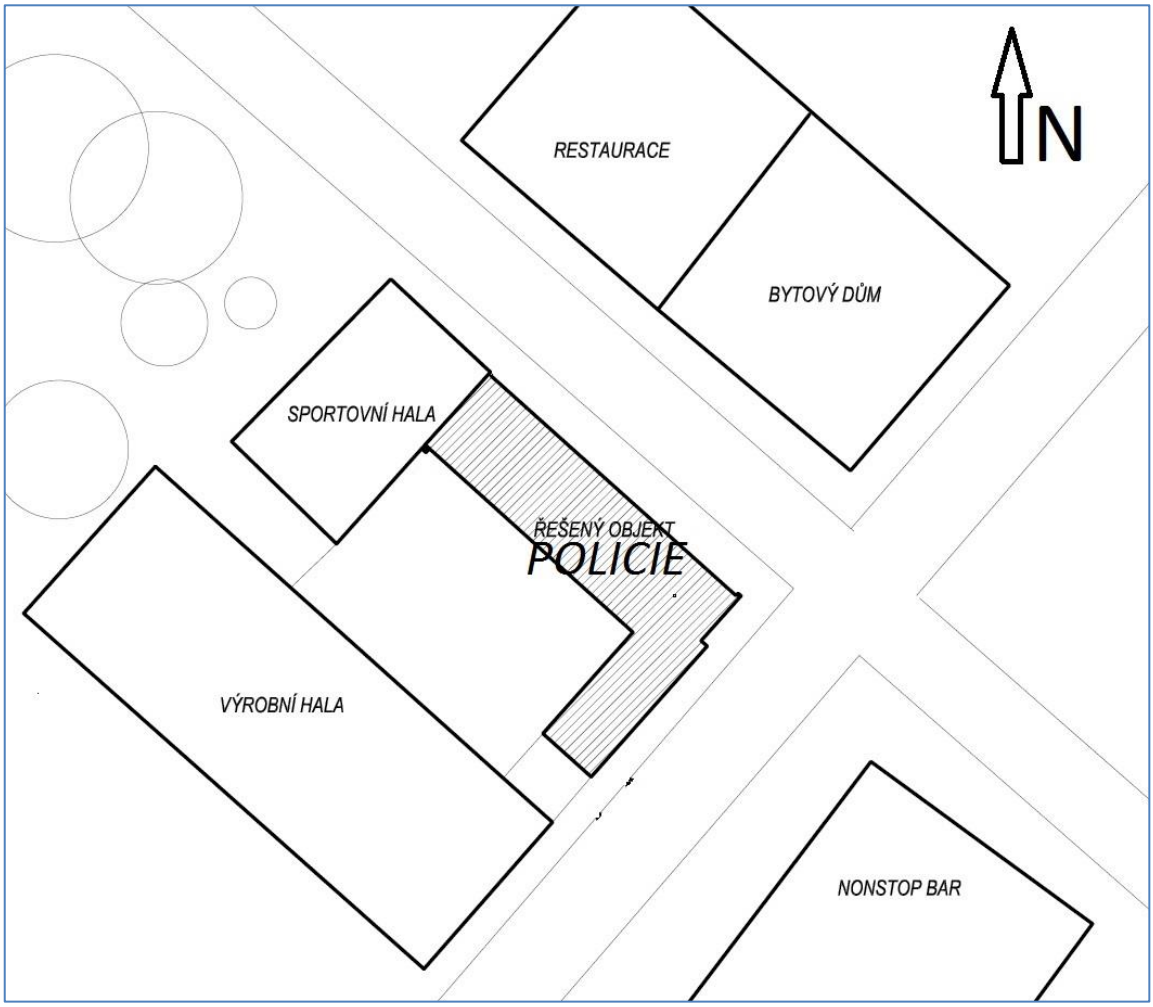
P 6 2NP severní křídlo budovy – zakreslení techniky

P 7 3NP severní křídlo budovy – zakreslení techniky

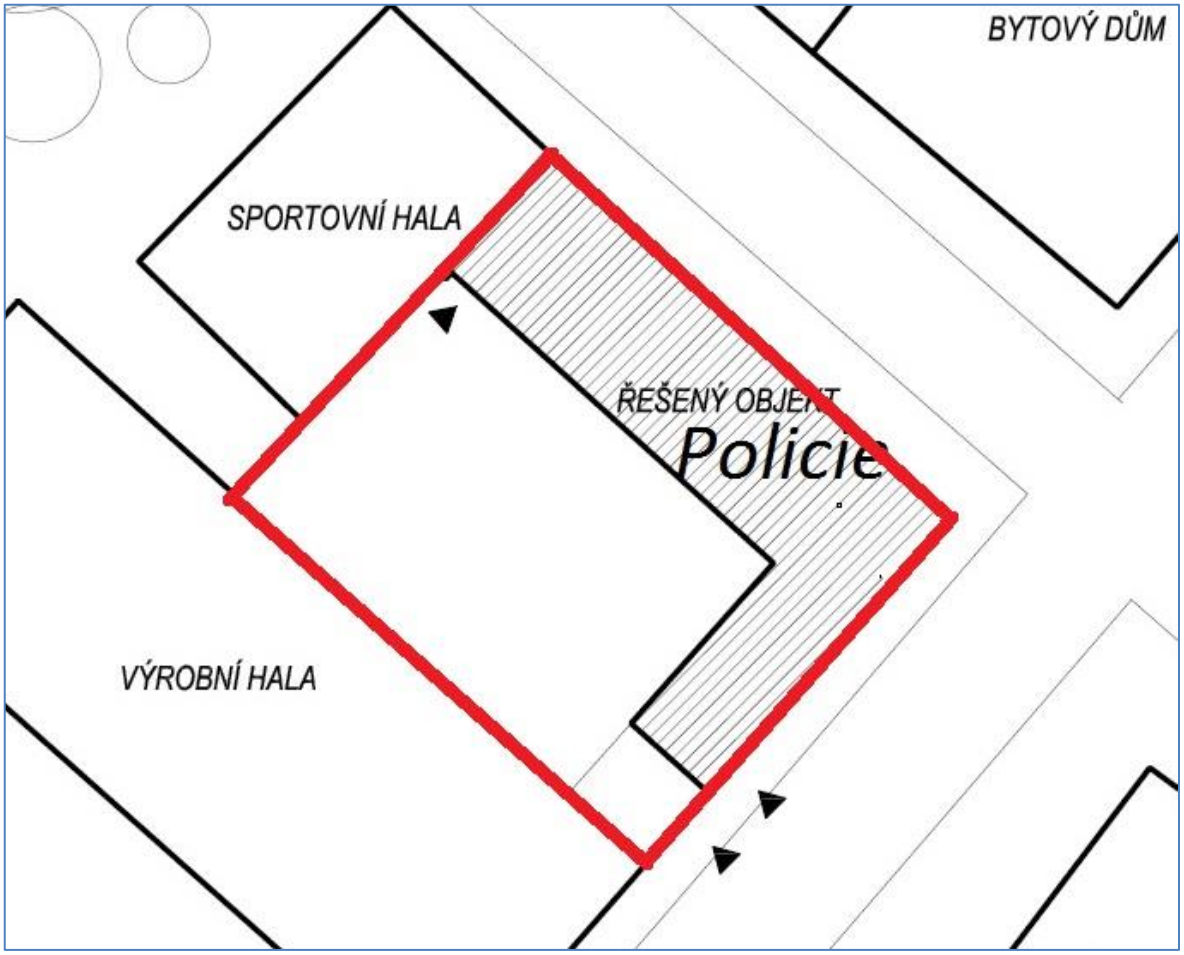
P 8 Zakreslení umístění kamer

P 9 Struktura integrovaného poplachového zabezpečovacího systému

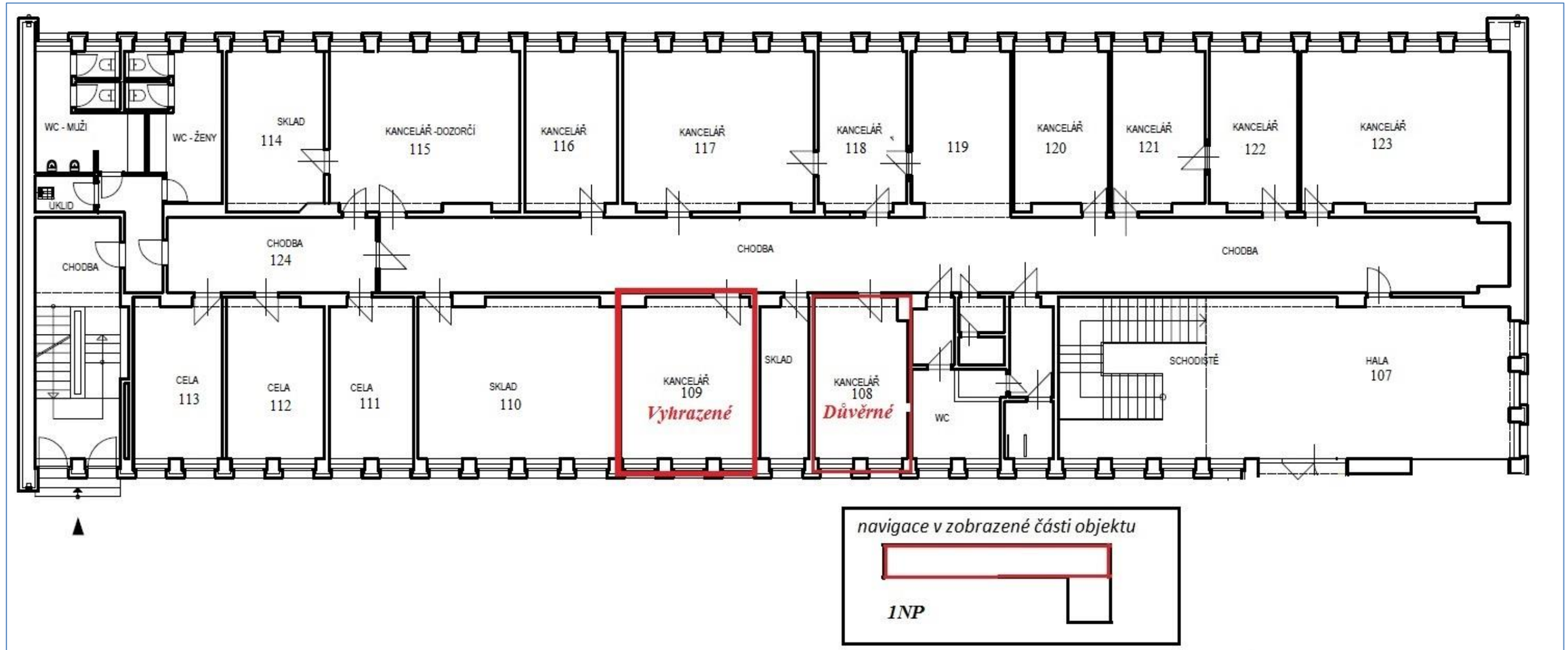
Příloha P 1: SITUACE ŘEŠENÉHO OBJEKTU



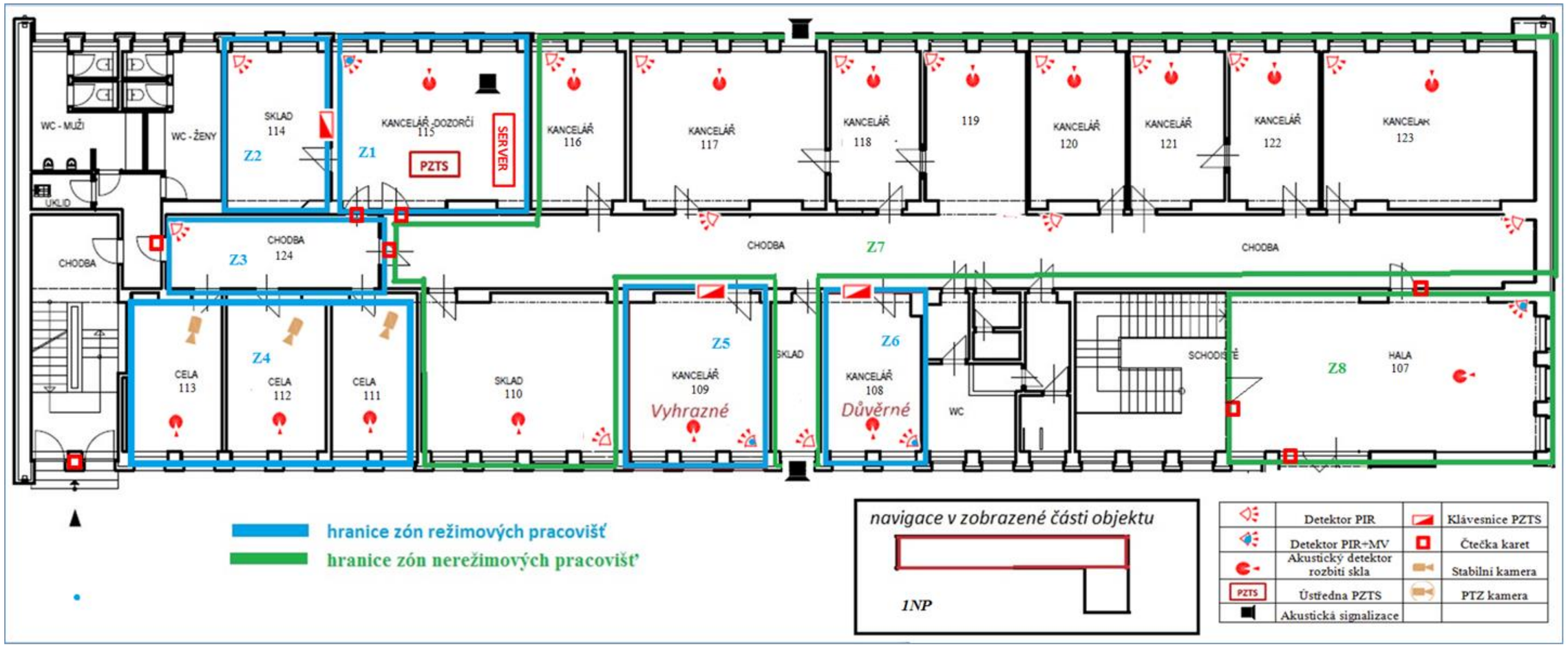
Příloha P 2: HRANICE ZABEZPEČENÉHO OBJEKTU Z HLEDISKA OUI



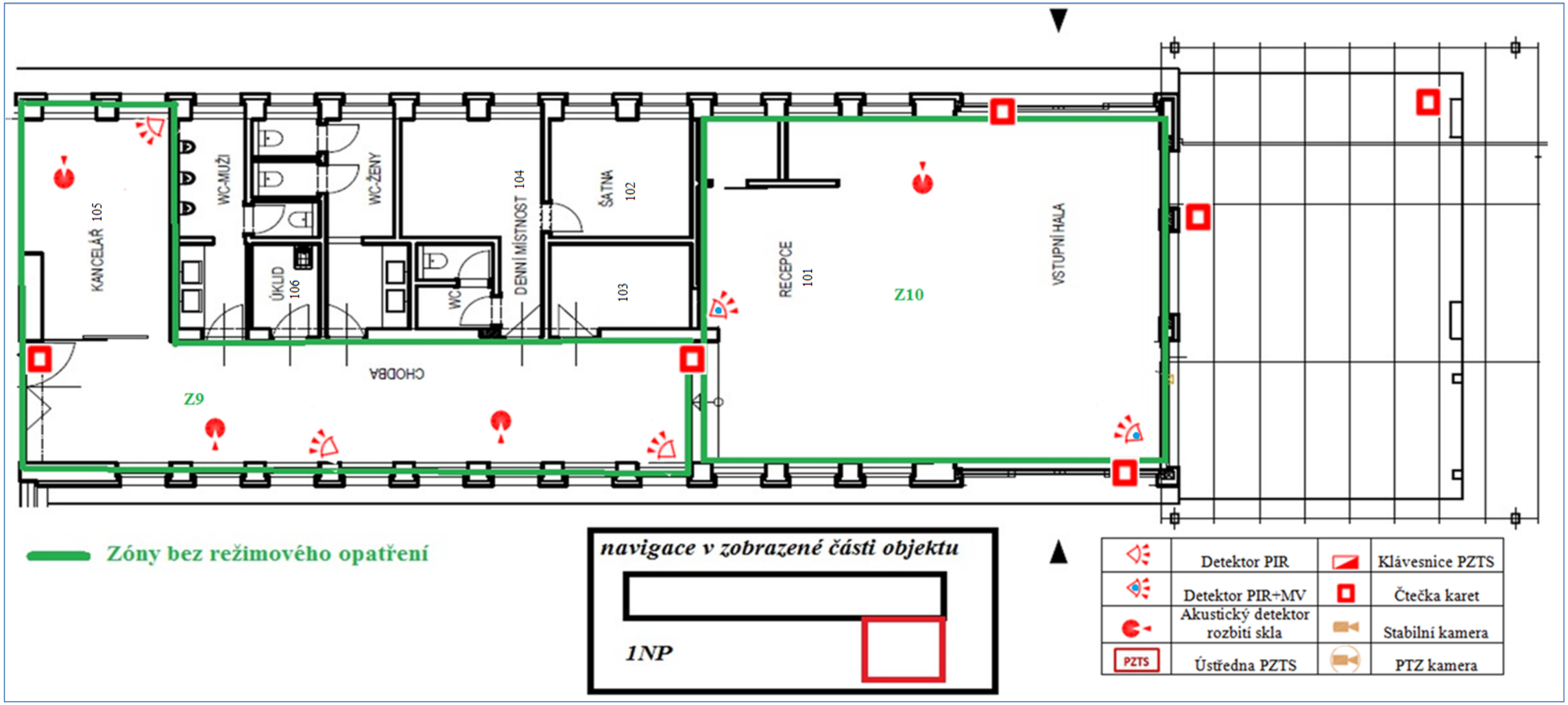
Příloha P 3: HRANICE ZABEZPEČENÝCH OBLASTÍ OUI – 1.NP



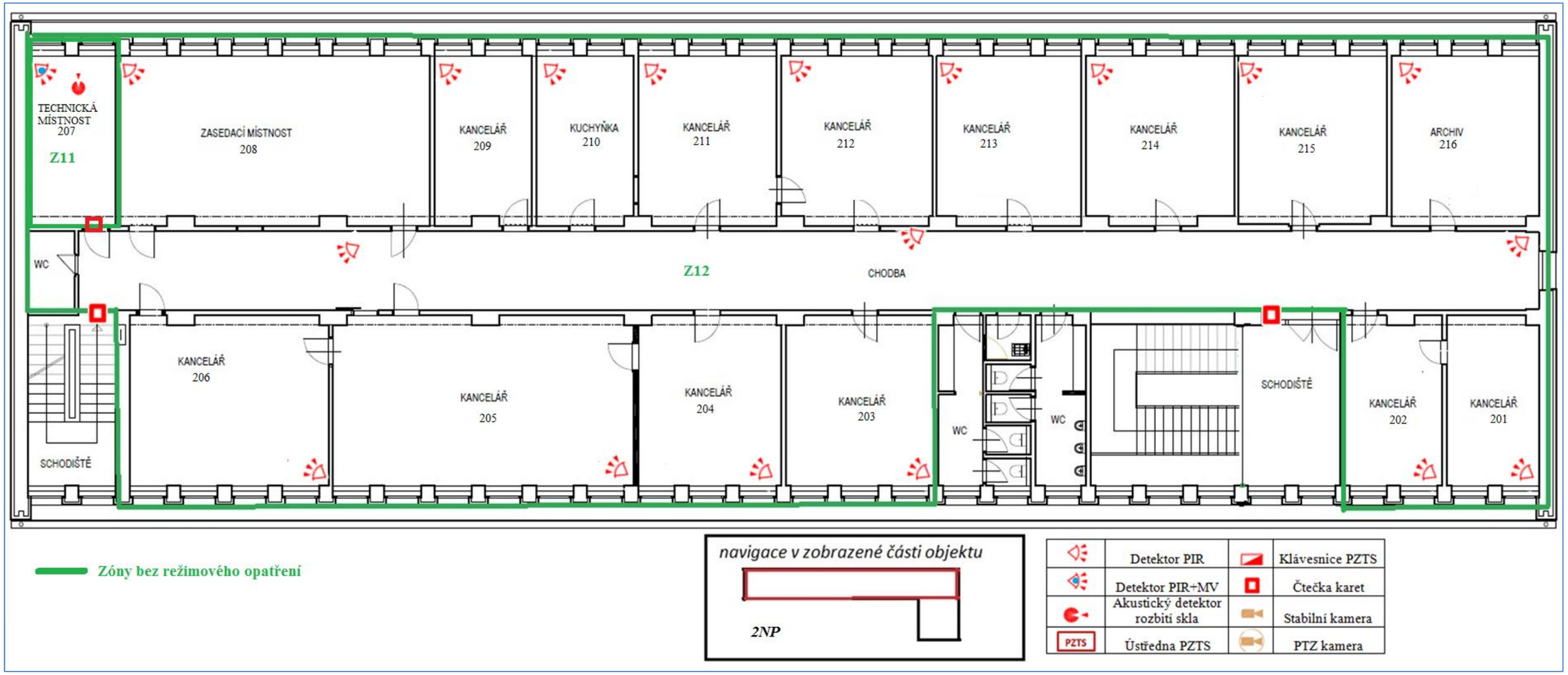
Příloha P 4: 1.NP SEVERNÍ KŘÍDLO BUDOVY – ZAKRESLENÍ TECHNIKY



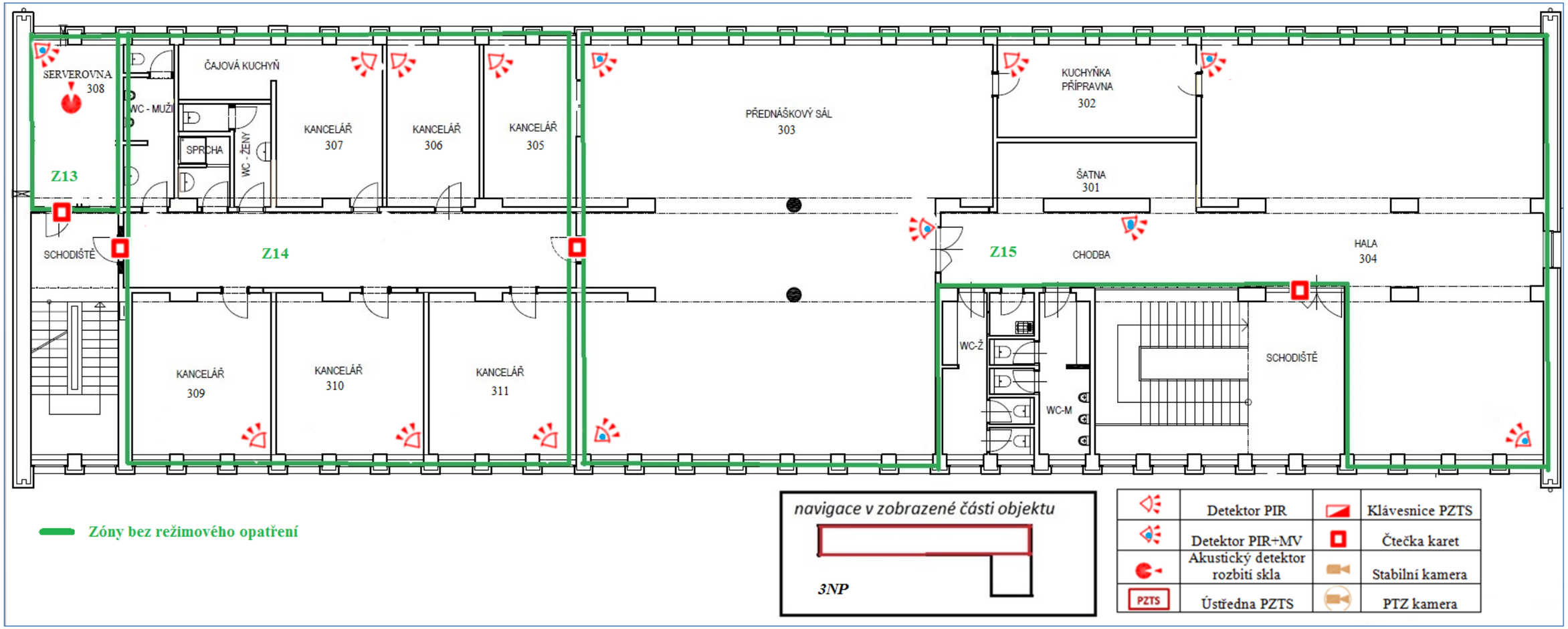
Příloha P 5: 1.NP ZÁPADNÍ KŘÍDLO BUDOVY – ZAKRESLENÍ TECHNIKY



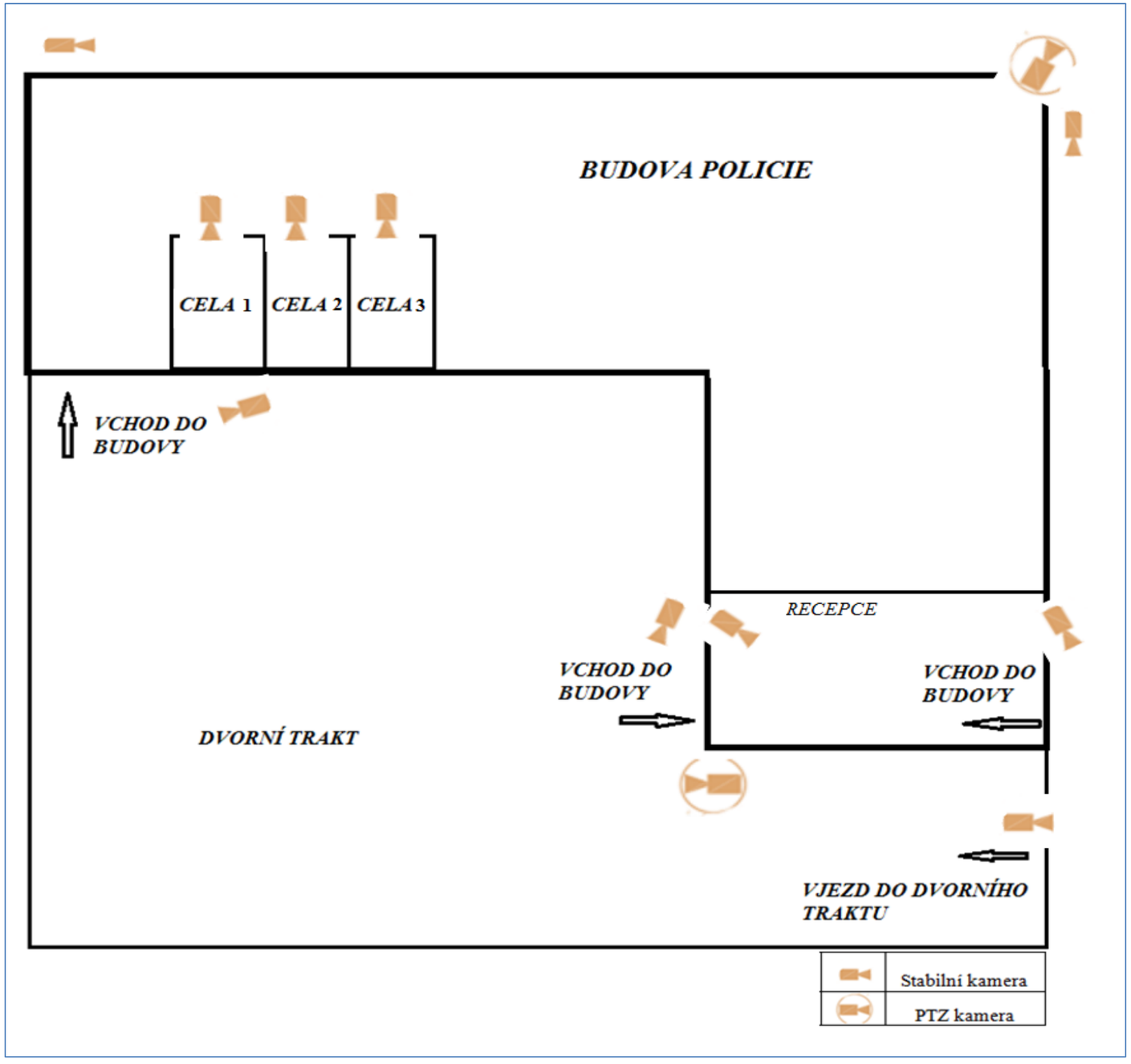
Příloha P 6: 2.NP SEVERNÍ KŘÍDLO BUDOVY – ZAKRESLENÍ TECHNIKY



Příloha P 7: 3.NP SEVERNÍ KŘÍDLO BUDOVY – ZAKRESLENÍ TECHNIKY



Příloha P 8: ROZMÍSTNĚNÍ BEZPEČNOSTNÍCH KAMER



Příloha P 9: STRUKTURA INTEGROVANÉHO POPLACHOVÉHO ZABEZPEČOVACÍHO SYSTÉMU