Zabezpečení sadu

Security of Orchard

Vojtěch Filipovič

Bakalářská práce
2013

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

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

Jméno a příjmení:	**Vojtěch FILIPOVIČ**
Osobní číslo:	**A09670**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Zabezpečení sadu**

Zásady pro vypracování:

1. **Proveďte analýzu stávajících elektronických bezpečnostních systémů pro zabezpečení perimetru.**
2. **Zpracujte normy a právní úpravy vztahující se k tématu bakalářské práce.**
3. **Proveďte bezpečnostní analýzu okolí a zhodnoťte rizika.**
4. **Na příkladu zabezpečení sadu navrhněte dvě vlastní varianty řešení.**
5. **Odhadněte další vývoj těchto systémů.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **IVANKA, Ján. Mechanické zábranné systémy. Zlín: UTB ve Zlíně, 2010. 151 s. ISBN 978-80-7318-910-5.**
2. **IVANKA, Ján. Systemizace bezpečnostního průmyslu. Zlín: UTB ve Zlíně, 2009. 123 s. ISBN 978-80-7318-850-4.**
3. **KŘEČEK, Stanislav. Příručka zabezpečovací techniky. 2. vyd. Cricetus, 2003, 351 s. ISBN 80-902-9382-4.**
4. **ČANDÍK, Marek. Technické prostředky bezpečnostního průmyslu. Zlín : UTB ve Zlíně, 2005. 117 s. ISBN 8073183285.**
5. **UHLÁŘ, Jan. Technická ochrana objektů : II. díl – Elektrické zabezpečovací systémy. Praha : PA ČR, 2005. 227 s. ISBN 80-7251-189-0.**
6. **LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management I. 1. vyd. Zlín: VeRBuM, 2011, 316 s. ISBN 978-808-7500-057.**
7. **KINDL, Jiří. Projektování bezpečnostních systémů I. Zlín: UTB ve Zlíně, 2007. 134 s. ISBN 978-80-7318-554-1**

Vedoucí bakalářské práce: **Ing. Hana Charvátová, Ph.D.**
Ústav automatizace a řídicí techniky

Konzultant: **Ing. Rudolf Drga**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **25. února 2013**

Termín odevzdání bakalářské práce: **30. května 2013**

Ve Zlíně dne 25. února 2013

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Bakalářská práce podává přehledný soupis možností zabezpečení sadu. Práce se skládá z 5 částí. V první části jsou vybrány typy detektorů a kamer, následně je popsán princip, na kterém pracují. V části druhé jsou zpracovány normy a právní úpravy týkající se této problematiky, ve třetí části se zabývám srovnáním jednotlivých typů detektorů a kamer. Ve čtvrté části jsou zpracovány dva projekty zabezpečení existujícího sadu. V poslední části jsou popsány možné směry dalšího vývoje těchto systémů.

Klíčová slova: Poplachové a zabezpečovací tísňové systémy,perimetrická ochrana, bezpečnostní ploty, CCTV, sad.

ABSTRACT

Bachelor thesis presents a comprehensive list of security options of an orchard. The thesis consists of 5 parts. In the first part are selected types of detectors and cameras, then there is described the principle on which they are working. In the second part are processed standards and legislation regarding this issue, in the third part I deal with the comparison of the various types of detectors and cameras. The fourth part deals with the two security designs of existing orchard. The last section discusses possible directions for further development of these systems.

Keywords: Intruder and Hold-up Alarm System, perimeterprotection, securityfences, CCTV, orchard.

Tímto bych chtěl poděkovat své vedoucí práce Ing. Haně Charvátové za pomoc při zpracovávání bakalářské práce, její odborné vedení a rady. Dále bych chtěl poděkovat své rodině za podporu při studiích.

Prohlašuji, že

- beru na vědomí, že odevzdáním 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 bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk 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 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 – 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 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 bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

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

Ve Zlíně …….…….

podpis diplomanta

OBSAH

ÚVOD

Současný stav zločinnosti a majetkové trestné činnosti vede k obavám o vlastní majetek ať už soukromý či firemní. Pro tento účel již nestačí vysoký plot, pevné dveře a mříže na oknech, neboli mechanické prvky ochrany, které pomohou pachatele odradit nebo jej po určitou dobu zdržet. Současné technické prostředky nabízejí použití elektronických prvků pro poplachovou zabezpečovací a tísňovou signalizaci a využití kamerových systémů.

Systémy, které dokážou detekovat nežádoucí událost, jsou stále více implementovány v zabezpečení majetku. Se stále rostoucími nároky na zabezpečení je nutné tyto systémy inovovat a to ve všech směrech. Současný rozvoj elektroniky a miniaturizace vytváří výborné podmínky pro vývoj nových a vylepšování starších systémů, které spadají pod hlavičku poplachových zabezpečovacích a tísňových systémů (PZTS) a kamerových systémů – Closed Circuit Television (CCTV). Tento inovační trend má rozhodně stoupající tendenci, což je, vzhledem ke stále vyšší poptávce po zabezpečení a větším nárokům pojišťoven stav, který nikoho nepřekvapí.

Cílem této práce je seznámit zájemce s problematikou zabezpečení venkovního prostoru – perimetru, dále pak rozdělením jednotlivých detektorů a kamer, stručně vysvětlit princip, na kterém pracují a nalézt nejoptimálnější možnosti zabezpečení.

I. TEORETICKÁ ČÁST

1 PROBLEMATIKA ZABEZPEČENÍ SADU

Objekty sadů mají několik charakteristik, které předurčují, jakým způsobem se bude přistupovat k jejich zabezpečení.

V první řadě je to místo a rozloha území, kde jsou umístěny stromky. Rozloha se pohybuje od několika metrů čtverečních až po desítky hektarů. Jedním z podstatných rysů je požadavek na bezobslužnost, vzhledem k relativní odlehlosti míst. Nejčastěji jsou situovány v okrajových částech měst a obcí, či úplně na samotě. S tím souvisí i nezbytné napojení na technickou infrastrukturu, včetně datového připojení, které slouží jako jedna z komunikačních tras pro vyvedení na dohledové a poplachové přijímací centrum (DPPC). Při volbě typu zabezpečení je důležité si uvědomit, že stromy mají různou výšku a tvar, které snižuje celkovou přehlednost zastřeženého území a zvyšuje možnost falešných poplachů.

Dalším ovlivňujícím faktorem jsou požadavky bank a pojišťoven, které nám již v prvopočátku výstavby definují, jakým způsobem má být objekt zabezpečen, některé z nich předepisují použití konkrétních bezpečnostních prvků. Charakteristickým rysem je pak požadavek na certifikaci použitých technologií, materiálů, prvků a odborný návrh jejich použití.

Z hlediska objektové bezpečnosti je sad ohraničený areál určité rozlohy, s definovaným plánem výsadby a vnitřních komunikací. Z hlediska možných druhů trestné činnosti rozlišujeme tyto na vandalismus, krádeže nebo sabotáže zaměřené na znehodnocení úrody v důsledku konkurenčního boje.

Základem budoucího kvalitního zabezpečení je podrobná analýza daného objektu a přilehlého okolí, stanovení bezpečnostních rizik, návrh opatření a projekt řešení. Důležitým předpokladem pro určení bezpečnostních rizik a návrh zabezpečení jsou znalosti možného typu útoku a také fáze, v jaké ho chceme detekovat.

Perimetrickou ochranu lze realizovat různými technologiemi, v závislosti na místních podmínkách a požadované úrovni zabezpečení. Pokaždé se však jedná o kombinaci několika prvků PZTS v kombinaci s mechanickými zábrannými systémy (MZS), také lze využít systémů CCTV. Při výběru technologie je důležité si uvědomit, že bezpečnostní systém by měl být nejen funkční a detekčně spolehlivý, ale musí také vykazovat minimum falešných poplachů, aby majiteli nepřidělával starosti a nezvyšoval také provozní náklady,

například za zbytečné výjezdy externí fyzické ostrahy, vykonávané většinou některou z bezpečnostních agentur.

Neopomenutelnou součástí je také fyzická ostraha objektu, která je potřeba zejména v prvopočátku, tedy v době výsadby a výstavby. Jakmile je do provozu spuštěna některá z ucelených částí zabezpečovacího systému, není většinou nutné, aby fyzická ostraha dále zůstávala na místě 24 hodin denně.

Pracovníci firmy, provádějící instalaci zabezpečovacích systémů, musí být proškolení k montáži použitých zařízení a tuto skutečnost prováděcí firma dokládá příslušným osvědčením. Na neodborné zapojení těchto zařízení se zpravidla nevztahuje záruka výrobce a rovněž dochází k případnému vyvinění pojišťovny z pojistného plnění v případě odcizení či jakéhokoliv poškození.

2 MOŽNOSTI ZABEZPEČENÍ SADU

Jedná se o zabezpečení perimetru, kde lze využít 4 možnosti zabezpečení ve formě mechanických zábranných systémů, poplachových a tísňových zabezpečovacích systémů, CCTV a přítomnosti fyzické ostrahy. [1].

2.1 Mechanické zábranné systémy

Mechanické zábranné systémy považujeme za základní prvek ochrany. Pod mechanické zábranné systémy řadíme veškeré mechanické prvky, které stěžují násilné vniknutí osob do chráněné zóny nebo objektu především skrz oplocení nebo cestou dveřních nebo okenních otvorů. Dále manipulaci nepovolané osoby s chráněnými předměty v zabezpečeném objektu. Hovoříme o tom, že mechanické zábranné systémy poskytují ochranu svou mechanickou pevností. Doba, kterou musí pachatel vynaložit na její překonání je v mnohých případech delší, než je pro pachatele únosné. Základní úlohou MZS je tedy vytvořit překážku definovanou určitým odporem proti destrukčnímu narušení[1].

2.1.1 Oplocení

Oplocení areálu patří do mechanických zábranných systémů perimetrické ochrany. Ohraničuje vymezený prostor areálu od okolního prostředí a tvoří hranici pozemku. Je realizováno z pevně osazených částí. Hlavním úkolem je zabránit narušení střežené oblasti ať už přelezením, podlezením či podkopáním. Součástí oplocení jsou vstupní prvky (brány), které musí být řádně ukotveny a musí splňovat stejné bezpečnostní požadavky jako oplocení[2].

Obrázek 1 Oplocení s vrcholovou zábranou[3]

Součásti oplocení může být i vrcholová zábrana, jejímž úkolem je ztížit narušiteli přelezení plotu. Vrcholové zábrany mají různou konstrukci i délku a jsou instalovány na vrchní části plotu. Zpravidla jsou umístěny na konzolách, připevněných na sloupcích oplocení pod úhlem 45 stupňů směrem od objektu, nebo majících tvar písmene Y. Na těchto prvcích je přichyceno několik řad samostatných, nebo navzájem spletených ostnatých nebo žiletkových drátů[2].

2.1.2 Vstupní brána

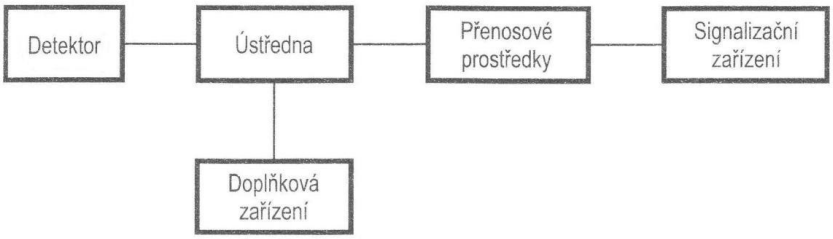
Vstupní brána, popřípadě branka je součástí oplocení a umožňuje osobám, případně vozidlům přístup do zabezpečeného prostoru. Brány můžeme dle způsobu otevírání dělit na posuvné nebo otočné s manuálním, nebo dálkovým ovládáním[2].

2.1.3 Bezpečnostní zámek vstupu

Na bráně může být zámek přímo jako součást křídla, případně může být jako visací. Tento zámek však musí splňovat požadovaný stupeň ochrany dle požadavků klienta. Bezpečnost je určena především profilem klíčového otvoru, členitostí klíče, použitých materiálů a bezpečnostními prvky proti odvrtání, ulomení a vytržení vložky ze zámku. U visacího zámku je potřeba, aby tento byl odolný vůči přestřižení, přeřezání, vytržení, nebo odvrtání tělese ze zámku. Konstrukce může být tvořena jednou nebo více vrstvami. U obou typů zámků je potřeba, aby splňovaly patřičnou bezpečnostní třídu, dle podmínek pojišťovny[2].

2.2 Poplachové zabezpečovací a tísňové systémy

Poplachový a tísňový zabezpečovací systém (Obr. 2) je soubor prvků schopných dálkově opticky a akusticky signalizovat na určeném místě přítomnost, vstup nebo pokus o vstup narušitele do střežených prostor. Každý poplachový a tísňový zabezpečovací systém je složen z několika základních prvků plnících své specifické funkce. Vytváří zabezpečovací řetězec. Patří sem detektor, ústředna, přenosové prostředky, signalizační zařízení a doplňková zařízení[4].



Obrázek 2Blokové schéma poplachového zabezpečovacího systému[4]

2.2.1 Ochrana plotu

Perimetrické plotové systémy se používají jako detekční systémy pro střežení obvodovou chráněného prostoru a to jako primární nebo doplňkové systémy. Tyto systémy umožňují chránit ploty z pletiva, prefabrikátů, dřevěných latí apod. U sadů se nejčastěji setkáme s žádným nebo pletivovým oplocením. Toto může být doplněno detekčním systémem senzorických kabelů, mikrofonních kabelů, kabelů na bázi optických vláken, nebo kapacitních kabelů. Tyto systémy zaznamenají a vyhodnotí narušení zábrany (plotu) v podobě přelezení, rozstřihnutí, podlezení a podkopání plotu, měly by však být odolné vůči planým poplachům vlivem silného deště a větru, krupobití, sněhové vánice, zvěře, ale také vůči elektromagnetickému a rádiovému rušení[4].

2.2.2 Infrazávory a bariéry

Infračervené závory a bariéry jsou jedny z nejrozšířenějších druhů perimetrické ochrany. Jsou aktivními prvky perimetrické ochrany a pracují na principu vysílače a přijímače mezi střeženým prostorem. Vysílač infrazávory a infrabariéry vysílá pomocí generátoru a vhodného optického zařízení, skládajícího se ze speciálních čoček, kódované infračervené paprsky. Na protilehlém místě je instalovaný přijímač, který paprsky přijímá. Přijímač komunikuje s řídící jednotkou, řízenou mikroprocesorem, a informuje ji o svém okamžitém

stavu. Při přerušení infračerveného paprsku nebo poklesu detekované úrovně, zapříčiněné vstupem do jeho dráhy, je vyhlášen poplach[4].

Součástí vysílačů jsou modulátory, které modulují světelný tok tak, aby šířka vlastních pulzů byla úzká a amplituda malá. Podle výrobce a typu se řádově pohybuje v jednotkách, až desítkách mikrosekund, mezera mezi jednotlivými pulzy se pohybuje v jednotkách milisekund. Toto opatření chrání infrazávory a infrabariéry proti oklamání, například jiným infračerveným vysílačem[4].

Infrazávory a infrabariéry vysílají více synchronizovaných paprsků, které je potřeba přerušit, aby byl vyhlášen poplach, a to z důvodu, abychom zamezili případným planým poplachům způsobené zvěří. Často bývají opatřeny krytem, případně vnitřním vyhříváním, aby nedocházelo k orosení optiky, nánosu vlhkosti, námrazy nebo sněhu. Délku přerušení paprsků lze nastavit v závislosti na ovlivňování paprsků povětrnostními a jinými vlivy[4].

Obrázek 3 Infrazávora[5]

2.2.3 PIR detektory

Pasivní infračervený detektor nevyzařuje do chráněného prostoru žádnou energii. Fyzikální princip činnosti passive infrared (PIR) detektoru spočívá ve snímání infračerveného spektra elektromagnetického záření (0,75 - 10 mikrometrů). Takto je detekováno teplotní záření v rozmezí teplot od -273°C do +560°C. Pro teplotu lidského těla, která je přibližně 35°C, je charakteristická vlnová délka o velikosti 9,3 - 9,4 mikrometrů. Záření je u PIR detektoru zachyceno pyroelementem, pracujícím na principu snímání rozdílné teplotní úrovně od normálu. Pohybuje-li se v chráněném prostředí takový objekt, jehož teplota je odlišná od okolního prostředí, PIR detektor zaznamená jeho pohyb a vyhodnotí ho jako poplach[6].

Obrázek 4 Venkovní PIR detektor[7]

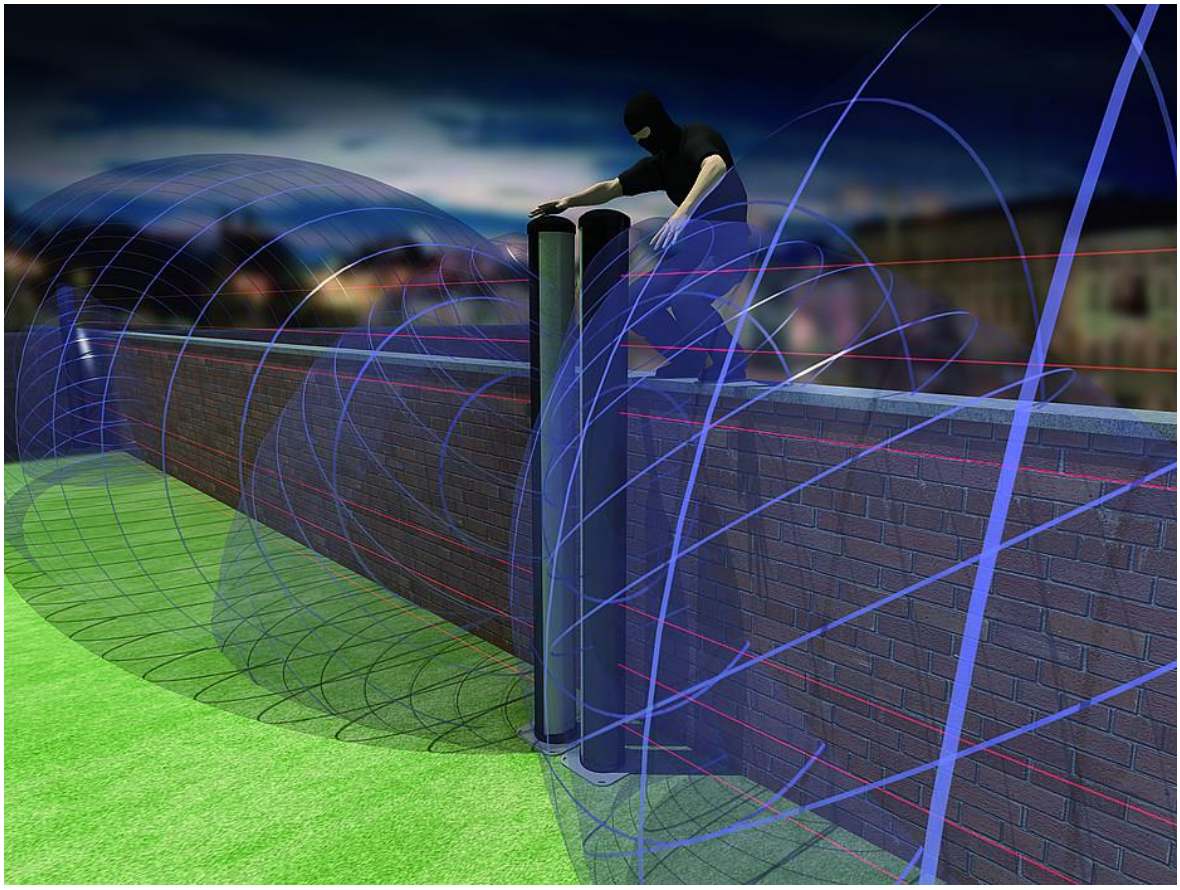
2.2.4 Mikrovlnné bariéry

Mikrovlnné bariéry vytvářejí vysokofrekvenční tvarované elektromagnetické pole mezi vysílačem a přijímačem. Tento systém detekuje a vyhodnocuje změny energie zachycené jeho přijímací anténou. Množství energie je ovlivňováno jak velikostí předmětů nebo osob, vyskytující se ve sledovaném prostoru, tak rovněž klimatickými podmínkami[4].

Nejčastějším tvarem mikrovlnného záření je rotační elipsoid s rotací kolem své osy. Pokud narušitel vstoupí do svazku mikrovlnného záření, bude toto vyhodnoceno jako poplach. Detekce narušení je zaručena i při částečném zastínění svazku mikrovlnného záření, při vzrůstu úrovně intenzity signálu nebo rušení jinými vysílači. Široký rozsah funkce automatického řízení umožňuje přijímači kompenzovat proměnlivost počasí i rozdílné podmínky instalace. Vzhledem k možnosti nastavení až 4 modulačních frekvencí jak ve vysílači, tak v přijímači, lze do jednoho pracovního prostoru umístit i více bariér. Pro detekování větších či menších cílů je zpravidla možno u těchto detektorů nastavit i citlivost. Pracují na frekvenci 2,5- 24 GHz a rozlišujeme několik typů s krátkým dosahem do 30 m, se středním dosahem kolem 150 m a s dlouhým dosahem až do 450 m[4].

Výhodou mikrovlnných bariér je široké rozpětí dosahu při relativně nejvyšší imunitě vůči povětrnostním vlivům. Vzhledem k tomu, že střežená zóna je vyplněna

elektromagnetickým vlněním, neexistuje pro narušitele ani teoretická možnost proniknout zabezpečenou zónou. Mikrovlnné bariéry jsou ideální pro střežení rozsáhlých ploch, jako jsou letiště, vojenské prostory, a také je lze využít v našem případě pro sadové areály[4].



Obrázek 5 Princip MW bariéry[8]

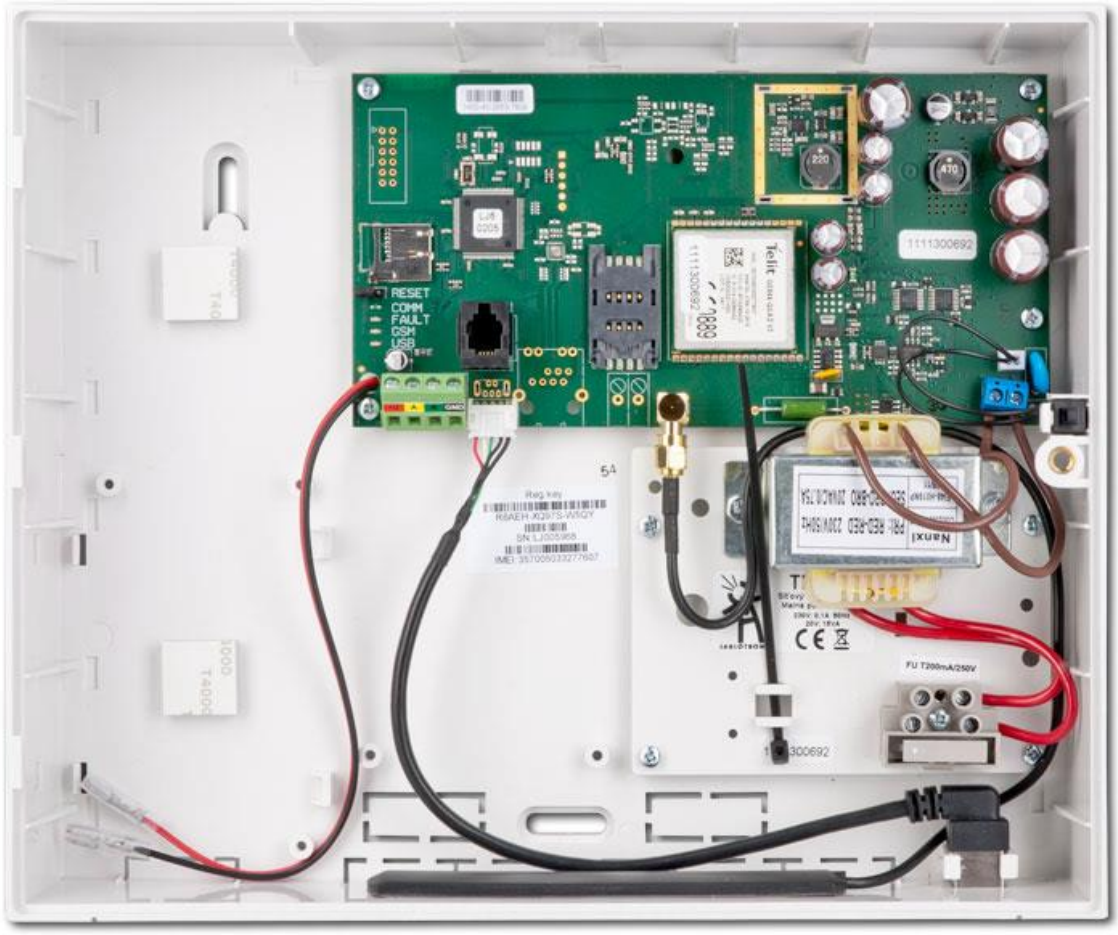
2.2.5 Duální PIR+MW detektory

Jedná se o pasivní infračervený detektor, který je kombinovaný s mikrovlnným detektorem. Mikrovlnná jednotka detekuje pohyb na základě odrazu mikrovlnné energie (Dopplerův efekt), zatímco pasivní infračervený detektor detekuje tepelné projevy pohybujícího se objektu. Pro vyhlášení poplachového stavu musí dojit k detekci v obou částech detektoru současně nebo ve velice krátkém časovém rozpětí. Mohou používat jako doplněk perimetrické ochrany. Detekční pole těchto detektorů jsou nastavitelná v závislosti na citlivosti mikrovlnného čidla a použité PIR čočky[6].

2.2.6 Ústředna PZTS

Ústředna PZTS je hlavním bezpečnostním prvkem. Jejím prvotním úkolem je přijímat a vyhodnocovat elektrické signály, přicházející od detektorů a dále v pravidelných

intervalech signalizovat a vysílat informace o svém stavu na DPPC a ovládat poplachové, signalizační a jiné doplňkové prostředky, které indikují narušení, nebo usnadňují činnost zásahové jednotky. PZTS ústředna komunikuje s DPPC pomocí telefonních linek, rádiových sítí nebo sítí Groupe Spécial Mobile (GSM). Pro lepší spolehlivost celého systému se často doporučuje použít také záložní komunikaci s DPPC[9].



Obrázek 6 Ústředna PZTS[10]

2.3 Kamerové systémy CCTV

Bezpečnostní kamery, vhodné pro zabezpečení sadu, můžeme rozdělit na dva druhy a to standardní a otočné Pan/Tilt/Zoom (PTZ) kamery. Kamery ve standardním provedení mají většinou tělo ve tvaru krabice. Kamery jsou obvykle osazené snímacím prvkem Charge-Coupled Device (CCD) a mají závit, na který se montuje objektiv s různými ohniskovými vzdálenostmi. Ten se volí na základě charakteristiky prostředí, do kterého bude kamera instalována a požadavků na parametry snímaného obrazu. Na zadní straně kamery bývají připojovací konektory pro přenos videosignálu, napájecí konektor, konfigurační spínače,

popřípadě alarmové vstupy a výstupy. Jelikož kamera je vystavována vnějším vlivům je nutné použít venkovní vyhřívaný kryt určený pro tyto účely. Otočné kamery neboli PTZ kamery jsou nejvíce univerzálními kamerami v sortimentu bezpečnostních kamerových systémů. Pomocí ovládací klávesnice či potřebného software můžeme kameru otáčet až o 360 stupňů a dle typu kamery použít také zoom, který může být například až 36x. Tyto vlastnosti umožňují uživateli sledování potřebných míst pomocí minimálního počtu kamer. Do kamery lze uložit takzvané prepozice, což v praxi znamená, že se kamera bude natáčet a sledovat přednastavené zájmové oblasti automaticky[11].

Obrázek 7Prvky CCTV systému[12]

Pro užití v bezpečnostním průmyslu rozlišujeme CCTV systémy na 4 základní skupiny[9].

2.3.1 Systém založený na PC

Patří k nejvyužívanějšímu řešení v oblasti počítačového zpracování obrazu. Pro uložení záznamu do PC je použita grabovací karta (tzv. Framegraber). Ta zajišťuje převod obrazového signálu do digitální podoby vhodné pro další zpracování v PC. Tyto karty jsou osazeny kompozitními a S-video vstupy. Ty mají horší kvalitu, ale pro nenáročné aplikace

jsou dostatečné. Karty jsou k dispozici v provedení PCI pro klasické i průmyslové PC. Ale také v provedení PXI pro připojení na sběrnici průmyslového PC[9].

Analogové karty dělíme do dvou kategorií. V první jsou použity kamery prokládaným řádkováním. Ve druhé jsou kamery s progresivním skenováním. Ty se vyznačují schopností vyčíst ze snímacího elementu v jednom okamžiku celý obraz (všechny řádky). Ty jsou vhodnější pro sledování rychle probíhajících dějů, jelikož poskytují vyšší rozlišení na snímek a tím více detailů. Samozřejmě mají také vyšší cenu. V dnešní době je ovšem výhodnější využít kamery s digitálním výstupem (Camera-link, FireWire 1394, USB) ty nevyužívají framegrabery. Kamerové systémy založené na PC jsou využívány hlavně v aplikacích, kde možnosti kompaktních systémů nestačí. Jsou to hlavně náročnější aplikace používající segmentaci obrazu, stereo vidění, více kamer[9].

Při volbě karty je potřeba brát ohled na typ vstupu zpracovávaného signálu, analogové rozhraní s normou Comittee Consultatif International Radiotelecommunique, Phase Alternate Line (CCIR PAL) nebo digitální rozhraní např. Camera-link, FireWire IEEE 1394[9].

2.3.2 Kompaktní systém

Jedná se o samostatnou jednotku s jednoúčelovým počítačem. Vzhledem ke své konstrukci jsou vhodné do prašných a jiným způsobem nepříznivých prostředí. Není vybaveno pevným diskem (HDD), proto jej lze využít i v prostředí s výskytem vibrací, které klasické HDD poškozují. Systém je vybaven velkým počtem vstupů a výstupů pro komunikaci s okolními zařízeními. Ke komunikaci s kamerou se obvykle používá sběrnice FireWire, k ní lze připojit větší množství kamer. Další komunikace je zajištěna pomocí RS 232 nebo přes ethernet. Pro připojení monitoru obsahuje systém výstup VGA. Mezi interní vybavení patří výkonný procesor, operační paměť (RAM) a paměť Flash, do ní je možné trvale uložit i několik testovacích programů. Hlavními světovými výrobci těchto systémů jsou firmy National Instrument a Panasonic[9].

2.3.3 Kamerový senzor

Jsou určeny především pro jednoduché průmyslové aplikace. Rozeznáváme dvě skupiny a to kamerové snímací hlavy s objektivem a snímací hlavy se závitem "CS mount". Jsou lehce konfigurovatelné přes PC a obsahují samo učící se funkce k zapamatování referenčního objektu. Přednosti jsou snadné nastavení a malé rozměry. Oblast použití je

zaměřena na jednoúčelové aplikace (detekce hran, kontrola rozměrů, třídění výrobků. Po zkonfigurování může snímací hlava pracovat samostatně bez kontroly přes monitor. Vývojem se zabývají firmy: Panasonic, Siemens, Sick[13].

2.3.4 Inteligentní kamery

Jedním z posledních trendů v oblasti bezpečnosti jsou inteligentní kamery. Jedná se o spojení kamery, vyhodnocovací a řídící jednotky a komunikačního rozhraní. Od nejjednodušších použití jako jsou měření velikosti, určení barvy, směru, rychlosti pohybu se dostávají kamery náročnějším operacím jako je detekce a rozpoznání objektu, využívané v dopravě, bezpečnostním průmyslu a v mnoha jiných odvětvích lidské činnosti. Tato funkce vyžaduje procesor. Ten vyhodnocuje jednotlivé objekty a porovnává je s předepsaným vzorem nebo skupinou vzorů. Tvorba těchto programů vyžaduje hlubší znalosti z oblasti počítačového vidění a programování, klade vysoké nároky na výpočetní výkon. Další funkce inteligentních kamer patří systém přesného zahájení snímání, to znamená pořídit snímek v přesně definovaném čase, bez ohledu na činnost kamery. K tomu je využit resetovaný režim kamery. Dále disponuje funkcí elektronické uzávěrky, kdy se změna expozice řídí změnou časování substrátových hodin senzoru CCD a Complementary Metal–Oxide Semiconductor (CMOS). Doby expozice, při využití elektronické expozice, se pohybují v rozmezí jednotek mikrosekund a desítek sekund. Při nákupu inteligentních kamer musíme počítat s vyšší cenou odvíjející se od jejich parametrů a schopností: velikost rozlišení, rychlost DSP (Digital Signal Processing), barevné hloubky, velikost a typ paměti, typ čipu, dostupného rozhraní, počtu I/O atd[9].

2.4 Fyzická ostraha

U tohoto typu střeženého areálu není příliš obvyklá, skládá se však většinou z bezpečnostního pracovníka – strážného, případně může být doprovázen psem (kynologická složka). Nejčastěji je realizována přes systém CCTV a pomocí pravidelných obchůzek po areálu. Výhodou tohoto způsobu je možnost prakticky ihned zasáhnout proti narušiteli, ovšem jako značná nevýhoda působí stále výdaje[14].

2.5 Režimová opatření

Do režimových opatření spadají různé administrativní a organizační pokyny ve formě směrnic a nařízení. Ovlivňují vstup do objektu, délku setrvání, pohyb vozidel, kontrolu při vstupu a výstupu a další požadavky dle přání klienta, nebo pojišťovny[14].

3 ZPRACOVÁNÍ POUŽITÝCH TECHNICKÝCH NOREM A PRÁVNÍCH ÚPRAV

Z důvodu normalizace technické stránky zabezpečení a legislativních ošetření ohledně využívání CCTV systému se budu v následující kapitole zabývat těmito náležitostmi.

3.1 Technické normy

Zde jsou shrnuty technické normy týkající možně použitých komponent při zabezpečování sadových areálů.

3.1.1 ČSN EN 50131-1 ed.2

Tato evropská norma, která je platná od 1. května 2007 stanovuje systémové požadavky poplachových zabezpečovacích a tísňových systémů.

3.1.1.1 Stupně zabezpečení

Norma ČSN EN 50131-1 člení prvky PZTS do čtyř stupňů zabezpečení, které uvádí tabulka 1. Míra rizika je stanovena předpokládanou vybaveností pachatele a jeho znalostí daného systému.

Stupeň	Míra rizika	Předpokládaný typ narušitele
1	nízké	Narušitel má malou znalost systému, omezený sortiment snadno dostupných nástrojů
2	nízké až střední	Narušitel má určitě znalosti systému
3	střední až vysoké	Narušitel je obeznámen se systémem, úplný sortiment základních přenosných přístrojů a elektronických zařízení
4	vysoké	Narušitel je schopen nebo má možnost zpracovat podrobný plán vniknutí

Tabulka 1 Stupně zabezpečení podle ČSN EN 50131-1 ed.2 [2]

3.1.1.2 Klasifikace prostředí

Při výběru komponentu PZTS je nutné dbát i na prostředí, ve kterém bude daný výrobek pracovat. ČSN EN 50131-1 rozlišuje 4 třídy prostředí (tabulka 2).

Třída	Název prostředí	Popis prostředí, příklady	Rozsah teplot
I	vnitřní	Vytápěná obytná nebo obchodní místa	+5°C až +40°C
II	vnitřní všeobecné	Přerušovaně vytápěná nebo nevytápěná místa (chodby, schodiště, skladové prostory)	-10°C až +40°C
III	venkovní chráněné	Prostředí vně budov, kde komponenty nejsou trvale vystaveny vlivům počasí (přístřešky)	-25°C až +50°C
IV	venkovní všeobecné	Prostředí vně budov, kde komponenty jsou trvale vystaveny vlivům počasí	-25°C až +60°C

Tabulka 2 Třídy prostředí dle ČSN EN 50131-1 ed.2[1]

3.1.2 ČSN EN 50132-7

Kamerové systémy jsou zařazeny mezi technické systémy umožňující automatické zpracování osobních údajů. Tím pádem podléhají zákonu č.101/2000 Sb. Přesnou definici kamerového systému udává norma ČSN EN 50132-7(poplachové systémy – CCTV sledovací systémy pro použití v bezpečnostních aplikacích.) „CCTV systém je systém obsahující kamerovou sestavu, zobrazovací a přídavná zařízení nezbytná pro přenos signálu a obsluhu při sledování definované bezpečnostní zóny“ [1].

Dále jsou v normě uvedeny termíny popisující kamerový systém:

- **(Video)monitor:** zařízení pro zobrazení videosignálu na obrazovce.
- Přijatelný obraz: obraz vytvářený kamerou za nízkého osvětlení, poskytující dostatečný kontrast, zatímco šum v obraze generovaný kamerou zůstává na specifikované úrovni.
- **CCTV kamerová sestava:** jednotka obsahující CCTV kameru (CCTV kamera je jednotka obsahující snímací prvek vytvářející z optického obrazu videosignál) s příslušným objektivem a nezbytným příslušenstvím.

- **Řídící jednotka CCTV:** řídící a monitorovací zařízení požadovaných provozních funkcí systému CCTV.
- **Horizontální rozlišovací schopnost:** míra schopnosti monitoru rozlišit obrazový detail ve směru řádku.
- **Záznam události:** řízený záznam, nebo uložení obrazového signálu na danou dobu.
- Vzorkovací záznam: periodický záznam televizního signálu v předem definovaných intervalech.
- **Multiplexní záznam:** metoda záznamu několika videosignálů do jednoho televizního kanálu pomocí časového přepínání snímků/půl snímků těchto videosignálů.

Díváme-li se na kamerový systém jako na celek je možné jej definovat takto. „Uzavřený televizní okruh v nejjednodušší formě je prostředek, který umožňuje zobrazovat obrazy snímané televizní kamerou na monitoru prostřednictvím vlastního přenosového systému. Počet kamer a monitorů v instalaci není teoreticky omezen, ale v praxi bude limitován zvolenou konfigurací řídícího pracoviště a schopností řídící obsluhy tento systém řídit[1].

3.1.3 ČSN EN 1627

Tato norma určuje požadavky a systém klasifikace vlastností odolnosti proti vloupání u dveří, oken, lehkých obvodových plášťů, mříží a okenic. Jedná se o náhradu normy ČSN P ENV 1627 a vyšla v platnost 1. února 2012.

Pyramida bezpečnosti

Obrázek 8 Pyramida bezpečnosti dle ČSN EN 1627[2]

Pyramida bezpečnosti je složena ze čtyř barevně odlišených stupňů zabezpečení. Jednotlivé stupně zabezpečení určují odolnost výrobků. Pyramida svým tvarem i popisem označuje, které zařízení je vhodné k základní, zvýšené, vysoké nebo velmi vysoké úrovni ochrany majetku. Jedná se o jednotící komunikační prvek, který usnadňuje a zpřehledňuje

identifikaci výrobků s ověřenou úrovní jakosti a je zaměřen výhradně na certifikované výrobky mechanických zábranných systémů[2].

3.1.4 Směrnice ČAP P 2333

Směrnice ČAP P 2333 požaduje v jednotlivých pojistných třídách A, B, C, D, E a F příslušné stavební konstrukce jištěného objektu a zde vždy uvádí [1]:

- Optimální provedení.
- Jiné varianty.
- Doporučení.

Směrnice se týká mechanických zábranných systémů, poplachových zabezpečovacích a tísňových systémů (PZTS), ale také jejich kombinací. Uvedená opatření vycházejí z předpisů a norem [1]:

ČSN EN 1627

- Okna, dveře, uzávěry – odolnost proti násilnému vniknutí – požadavky a klasifikace.

ČSN EN 50131-1

- Poplachové systémy – elektrické zabezpečovací systémy, část 1 všeobecné požadavky.

ČAP P 131-7

- Poplachové systémy, elektrické zabezpečovací systémy, aplikační směrnice.

Směrnice ČAP má pouze charakter doporučení a pojišťovací společnosti mohou používat jiné předpisy řešící tuto problematiku při pojištění objektu.

	Pojistné třídy					
	A	B	C	D	E	F
ČSN EN 1627	2	3	3	4	5	6
ČSN EN 50131-1	2*	2	3	3	4	4
ČAP P 131-7	1*	2	2	3	4	4

Tabulka 3 Pojistné třídy podle směrnice ČAP 2333[1]

3.2 Právní úpravy

Po zpracování technických norem je potřeba znát i právní ustanovení ohledně monitorování areálu, které je zpracováno dále.

3.2.1 Zákon č. 101/2000 Sb.

3.2.1.1 Kamerový systém a lidská práva

V problematice ochrany základních práv a svobod jedince je potřeba především vycházet z Listiny základních práv a svobod „Každý má právo aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno. Každý má právo na ochranu před neoprávněným zásahem do soukromého a osobního života. Každý má právo před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě“[15].

Od 4. dubna 2000, kdy byl v souladu s právem Evropských společenství přijat “Zákon” o ochraně osobních údajů a zřízen „Úřad" pro ochranu osobních údajů. Na veškeré zpracovávání osobních údajů, ať k němu dochází automatizovaně nebo jinými prostředky (vyjma zpracování osobních údajů, které provádí fyzická osoba výlučně pro osobní potřebu) je potřeba pohlížet podle znění tohoto zákona. U kamerových systémů je průnikem nedotknutelnosti osobního soukromí a techniky fakt, že lidské tělo je považováno za množinu automaticky zpracovatelných informací, které lze nejen uchovávat, ale následně porovnávat navzájem i s jinými soubory relevantních dat (jedinec může tedy být jako izolované individuum permanentně sledován, aniž si je toho vědom). Výsledkem je konstatování, že záznam z kamerového systému je podle českého právního řádu osobním údajem ve smyslu ustanovení § 4 písm. a) zákona b.101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů[15].

3.2.1.2 Základními pojmy ve vztahu ke kamerovým systémům:

- **Osobní údaj:** jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.

- **Citlivý údaj:** osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu.
- **Subjekt údajů:** fyzická osoba, k níž se osobní údaje vztahují.
- **Zpracování osobních údajů:** jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace.
- **Shromažďování osobních údajů:** systematický postup nebo soubor postupů, jehož cílem je získání osobních údajů za účelem jejich dalšího uložení na nosič informací pro jejich okamžité nebo pozdější zpracování.
- **Správce osobních údajů:** každý subjekt, který určuje účel, prostředky, zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak.
- **Zpracovatel osobních údajů:** každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona. Zveřejněný osobní údaj: osobní údaj zpřístupněný zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu.
- **Datový soubor:** jakýkoliv soubor osobních údajů uspořádaný podle společných nebo zvláštních kritérií.
- **Informační povinnost:** povinnost správce informovat subjekt údajů o podrobnostech jejich zpracování.
- **Oznamovací povinnost:** povinnost potenciálního správce osobních údajů písemně oznámit Úřadu před zpracováváním osobních údajů úmysl zpracovávání nebo stávajícího správce změnit registrované zpracování zákona.
- **Počátek zpracovávání:** po registraci systému Úřadem nebo 31. den ode dne doručení oznámení o zahájení zpracovávání (poznámka: toto platí v případě, že oznámení obsahovalo všechny náležitosti a že z oznámení nevznikla důvodná obava, že při zpracování osobních údajů by mohlo dojít k porušení zákona) na úřad.

- **Registrační číslo:** počítačem generované číslo, které je přiděleno registrovanému správci a pod kterým je evidován v registru zpracování vedeném Úřadem (poznámka: informace zapsané do registru, kromě popisu způsobu zpracování osobních údajů a popisu opatření k zajištění ochrany osobních údajů, jsou ze zákona veřejně přístupné. Veřejný registr zpracování osobních údajů je k dispozici na www.uoou.cz v rubrice Veřejný registr zpracování) [15].

3.2.1.3 Základní povinnosti správce

Platí-li vše výše uvedené, lze konstatovat, že osoba tzv. správce kamerového systému je jedna z klíčových pro jeho provoz. U obvyklých, státní správou schválených, a tedy právně závazných dokumentů předcházejících reálnému nasazení kamerového systému (kromě norem to mohou být například také vyhlášky – nejblíže našemu tématu je to například vyhláška č.499/2006 Sb., vyhláška o dokumentaci k realizaci staveb) nedošlo doposud k doplnění příslušných odkazů na již zmíněnou ochranu práv a svobod. Z tohoto důvodu můžeme pro vyjmenování základních zákonných povinností správce z hlediska instalace kamerového systému považovat ty, které jsou stanoveny v § 5 odst. 1 a odst. 2; §10; § 11odst. 1 a 5; § 13 a § 16 zákona č.101/2000 Sb., o ochraně osobních údajů[15].

Dle § 5 odst. 1 zákona je správce povinen:

a) stanovit účel, k němuž mají být osobní údaje zpracovány

   Poznámka: Doporučujeme při zvažování účelu kamerového systému vzít v potaz všechna stanoviště (všechny kamery).

b) stanovit prostředky a způsob zpracování osobních údajů
c) zpracovat pouze přesné osobní údaje, které získal v souladu s tímto zákonem
d) shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu
e) uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování.

   Poznámka: Doba uchovávání záznamů by tedy měla být stanovena tak, že nepřesáhne dobu potřebnou k tomu, aby incident zaznamenaný kamerou bylo možné dále prošetřit a zajistit nezbytné informace. Toto lze učinit při provozu systému s 24hodinovoubezpečnostní službou obvykle následující den po zjištění. V případě, že budova není o víkendu využívána, pak nejpozději třetí den po incidentu. Při provozu kamerového systému bez stálé

bezpečnostní služby je ale potřeba počítat s dobou nezbytně nutnou v délce sedmi až deseti kalendářních dní.

f) zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny
g) shromažďovat osobní údaje pouze otevřeně
h) nesdružovat osobní údaje, které byly získány k rozdílným účelům

Dle § 5 odst. 2,4 a § 10zákona může správce osobních údajů zpracovávat osobní údaje pouze se souhlasem subjektu údajů; bez tohoto souhlasu je může zpracovávat pouze v případech uvedených v § 5 odst. 2 písm. a) až g) zákona[15].

Dle § 11 odst. 1 a 5 zákona má správce povinnost vždy při shromažďování osobních údajů informovat subjekt údajů o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovávány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny, nejsou-li subjektu údajů tyto informace již známy (například v době získávání souhlasu jako informovaného projevu vůle). Dále jej musí informovat o jeho právu přístupu k osobním údajům, právu na opravu osobních údajů, jakož i o dalších právech stanovených v § 21 zákona. Při zpracování prováděném na základě výjimky zakotvené v § 5 odst. 2 písm. e) zákona nemusí být informační povinnost splněna pokaždé před zahájením zpracování v plném rozsahu; správce je v této situaci na základě § 11 odst. 5 zákona povinen informovat subjekt údajů o zpracování jeho osobních údajů bez zbytečného odkladu[15].

Dle § 13 odst. 1 a 2 zákona je správce povinen přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Dále je správce povinen zpracovat a dokumentovat přijatá a provedená technickoorganizační opatření k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy.

Dle § 16 zákona je správce povinen ještě před zahájením zpracovávání dat prostřednictvím kamerového systému oznámit zamýšlené zpracování osobních údajů Úřadu[15].

3.2.1.4 Oznamovací povinnost

Podle § 16 odst. 1 zákona je ten, kdo hodlá jako správce zpracovávat osobní údaje nebo změnit registrované zpracování podle tohoto zákona (s výjimkou zpracování uvedených v § 18) povinen tuto skutečnost písemně oznámit Úřadu před zpracováváním osobních údajů.

Oznamovací povinnost je díky přetrvávající nedůvěře ke státní správě jednou ze základních okolností, proč není názor provozovatelů bezpečnostních systémů na zákon č.101/2000 Sb. pozitivní. Považují ho za diktát státu, který si pro naplnění hesla pomáhat a chránit udělil množství výjimek, a provozování lokálních kamerových systémů označuje za invazivní). Druhou okolností podvědomého strachu ze splnění oznamovací povinnosti je doba nedávná, tzv. doba totality. Ačkoli můžeme v některých detailech vidět podobnost evidovaných údajů, jedná se dnes na rozdíl od minulosti, kdy v příslušné dokumentaci byly uvedeny po splnění oznamovací povinnosti údaje jako například: Informátor: Petr / Místo: Talisman / Zájmová osoba: Kratochvíl / Zpracoval: Lodník o informování podle demokratických zákonů uznávaných v mezinárodním kontextu[15].

Zákon 101/2000 Sb. ukládá Úřadu pro ochranu osobních údajů povinnost vést registr zpracování osobních údajů [§ 29 odst. 1 písm. b) zákona], a rovněž povinnost učinit registr veřejně přístupným (§ 35 odst. 2 zákona), s výjimkou informací uvedených v § 16 odst. 2 písm. e) a i) zákona. Oznámené zpracování zapsané do registru obsahuje:

- identifikační údaje správce,
- účel / účely zpracování,
- kategorie subjektů údajů a osobních údajů, které se těchto subjektů týkají zdroje osobních údajů,
- místo nebo místa zpracování osobních údajů,
- příjemce nebo kategorie příjemců a předpokládaná předání osobních údajů do jiných států.

Registr tím, že je veřejnosti otevřený, umožňuje přesvědčit se, zda určitá právnická nebo fyzická osoba zpracovává osobní údaje a zda splnila svou zákonnou povinnost takové zpracování oznámit Úřadu postupem podle § 16 zákona (pokud se na ni oznamovací povinnost vztahuje). V registru je možné vyhledávat podle názvu subjektu, přiděleného registračního čísla[15].

Doporučení: aby si každý provozovatel kamerového systému podle ní zpracoval vlastní provozní manuál, a tím jasně deklaroval zabezpečení osobních údajů osob před jejich zneužitím, se zčásti můžeme držet při rozhodování o oznamovací povinnosti. I zde by mohlo chybné rozhodnutí být posuzováno jako porušení zákona a bylo by na místě obávat se šetření a v krajním případě i postihu. Jediným způsobem, jakým si lze prakticky ověřit,

jestli je provozování každého konkrétního kamerového systému v souladu se zákonem č. 101/2000 Sb., o ochraně osobních údajů, je podstoupení procesu registrace[15].

3.2.1.5 Stanoviska

Z předchozích odstavců je více než patrné, že budoucnost provozování bezpečnostních systémů založených na principu cílené identifikace (například přístupové a kamerové systémy) se nenávratně posouvá z technického oboru do právního. A tak jako není v dnešní době možné postavit multifunkční budovu bez zohlednění hygienických a požárních předpisů, lze předpokládat, že realizace takovýchto systémů bude už v samém počátku muset bezpodmínečně vycházet také z práva na soukromí. Objektivní posouzení vývoje, ale ani odhad, jestli dojde v blízké či daleké budoucnosti k naplnění některé z vizí tzv. „eroze soukromí" a naplní se slova Georgie Orwella (1984 [16]: „Ať je kdekoli, ať spí či bdí, pracuje či odpočívá, ať je v posteli či ve vaně, může být sledován bez varování, aniž ví, že je sledován“) nebo Anthonyho Burgesse (1985 [17]: „Žádná taková povinnost už neexistuje, to přece víš. Existují jenom práva. Výbor pro lidská práva – to dává smysl. Výbor pro lidské povinnosti to je pitomý nesmysl, ne? Vždycky to byl nesmysl, a ty to víš.“), nejsou dnešním správcům kamerových systémů nic platné, to co potřebují, jsou konkrétní návody, ze kterých by při řešení svých problémů vycházeli. Čerpat můžeme ze zdrojů, na základě jejichž obsahu vznikl tento příspěvek[15].

Státní správu zde zastupují stanoviska Úřadu pro ochranu osobních údajů a k dnešnímu dni jsou dostupná jeho následující stanoviska, komentáře a vyjádření:

- Stanovisko č.1/2006: Provozování kamerového systému z hlediska zákona o ochraně osobních údajů.
- Stanovisko č.8/2006: K využívání elektronických karet".
- „Vyjádření a doporučení ÚOOÚ k možnosti instalovat kamerový systém v prostorách školy: 3/2007.

Čeho se týkají změny plnění registrační povinnosti:

- Stanovisko č.1/2008: Umístění kamerových systémů v bytových domech.
- Stanovisko č.2/2008: K možnosti obcí provozovat kamerový systém se záznamem na veřejných prostranstvích.

3.2.1.6 Informační povinnost

Podle § 11 odst. 1 zákona je správce při shromažďování osobních údajů povinen subjekt údajů informovat o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny, nejsou-li subjektu údajů tyto informace již známy. Správce musí subjekt údajů informovat o jeho právu přístupu k osobním údajům, právu na opravu osobních údajů, jakož i o dalších právech stanovených v § 21 (Ochrana práv subjektů údajů). Jedním z častých problémů, který trápí každého registrovaného provozovatele kamerového systému, je splnění povinnosti správce informovat subjekt údajů o zpracování jeho osobních údajů bez zbytečného odkladu. V případě prakticky každého kamerového systému se subjekt údajů dostane do záběru minimálně jedné z kamer dříve nežli ke správci samotnému. Obvykle vzhledem k monitorovanému objektu existují dvě odlišné skupiny subjektů údajů, a s tím pochopitelně také i rozdílná úroveň informací pro tyto skupiny osob[15].

U „pravidelných" návštěvníků (zaměstnanci, obyvatelé) je nejjednodušším způsobem splnění informační povinnosti například využití interního firemního procesu obsílkou, svolání shromáždění společenství vlastníků jednotek. V obou případech s následným vyvěšením nebo rozesláním zápisu jednání shromáždění všem zaměstnanců nebo obyvatelům, a to ještě před zahájením zpracování a v plném rozsahu požadovaném zákonem. Okruh subjektů údajů je v těchto případech správci předem znám, a ten má tak možnost je bez zbytečného odkladu informovat ještě před zahájením shromažďování údajů. U nepravidelných návštěvníků (návštěvy, náhodní kolemjdoucí), kteří se do záběru kamerového systému dostanou víceméně náhodně, je správce povinen splnit informační povinnost např. umístěním informačních tabulek u vstupu do sledovaných prostor. Tabulka musí obsahovat informace, kde bude subjektu údajů poskytnuta informace o zpracování v rozsahu požadovaném zákonem (tzn. kde si může například vyzvednout v písemné podobě další informace o kamerovém systému). Požádá-li subjekt o další informaci týkající se zpracování svých osobních údajů, je mu správce povinen (kromě jiného také se zohledněním § 12 odst. 3 zákona) tuto informaci bez zbytečného odkladu poskytnout[15].

3.2.1.7 Informační cedule

TENTO PROSTOR JE MONITOROVÁN KAMEROVÝM SYSTÉMEM, tak zní základní text na informační ceduli, kterou ve schválené podobě (mimo jiné i s ohledem na vyhlášky

týkající se dopravního značení – s prováděcí vyhláškou č. 193/2006 Sb.), jehož výrobu zajišťuje od července letošního roku Asociace technických bezpečnostních služeb Grémium Alarm. V současné době je informační cedule ve dvou základních podobách jako samolepka a jako dopravní[15].

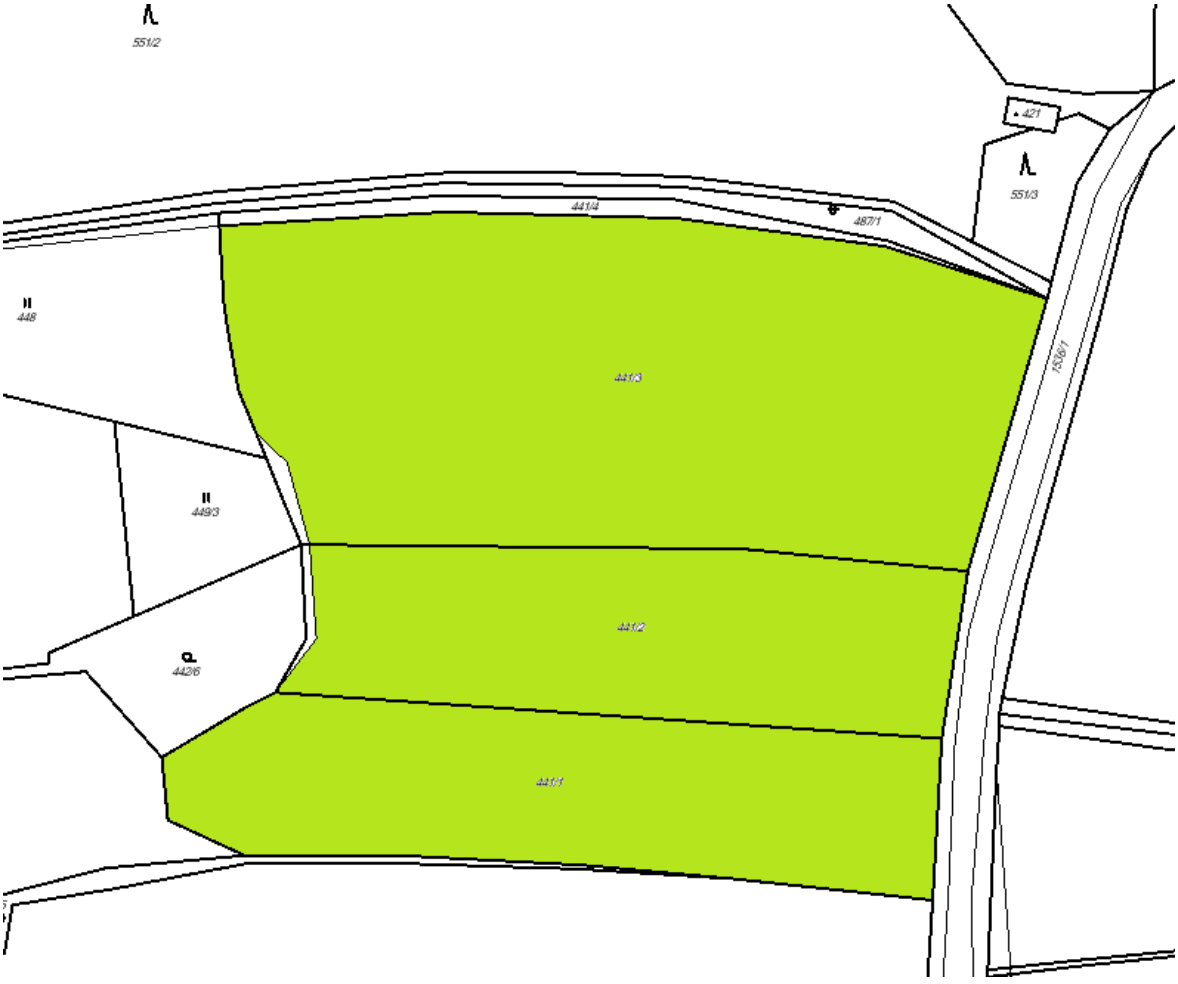
Obrázek 9 Informační cedulka[18]

Pro bytové domy a řadové objekty jsou k dispozici samolepicí štítky ve formátech A6; A5; A4. Štítky jsou určeny pro umístění po obvodu a u vchodů do objektu. Jejich instalace by měla být provedena tak, aby byl subjekt údajů upozorněn na skutečnost, že vstupuje do monitorovaného prostoru tomu je potřeba podřídit kromě umístění také velikost štítku. Vzhledem k tomu, že informační povinnost je potřeba splnit také u rozsáhlejších objektů (například u průmyslových podniků a komerčních zón), ale také u provozovatelů státem realizovaných nebo provozovaných kamerových systémů, tedy i u měst a obcí, jsou k dispozici také dopravní informační značky o rozměrech 700 x 500 mm. V září proběhla instalace podél vjezdových komunikací do prvních dvou obcí s nainstalovaným městským kamerovým dohlížecím systémem. K náležitostem této informační cedule, podmínky platí shodně pro samolepku i značku, je potřeba dodat, že musí obsahovat informaci, že prostor je sledován kamerovým systémem, musí zde být uveden správce provozovatel kamerového systému, resp. kontaktní osoba nebo sdělení, kde bude subjektu údajů poskytnuta informace o zpracování v rozsahu požadovaném zákonem (tj. kde si může např. vyzvednout v písemné podobě další informace o kamerovém systému). Vyplněný a takto umístěný štítek odpovídá zveřejněným stanoviskům Úřadu na ochranu osobních údajů k informační povinnosti správce kamerového systému[15].

II. PRAKTICKÁ ČÁST

4 BEZPEČNOSTNÍ ANALÝZA AREÁLU SADU A JEHO OKOLÍ

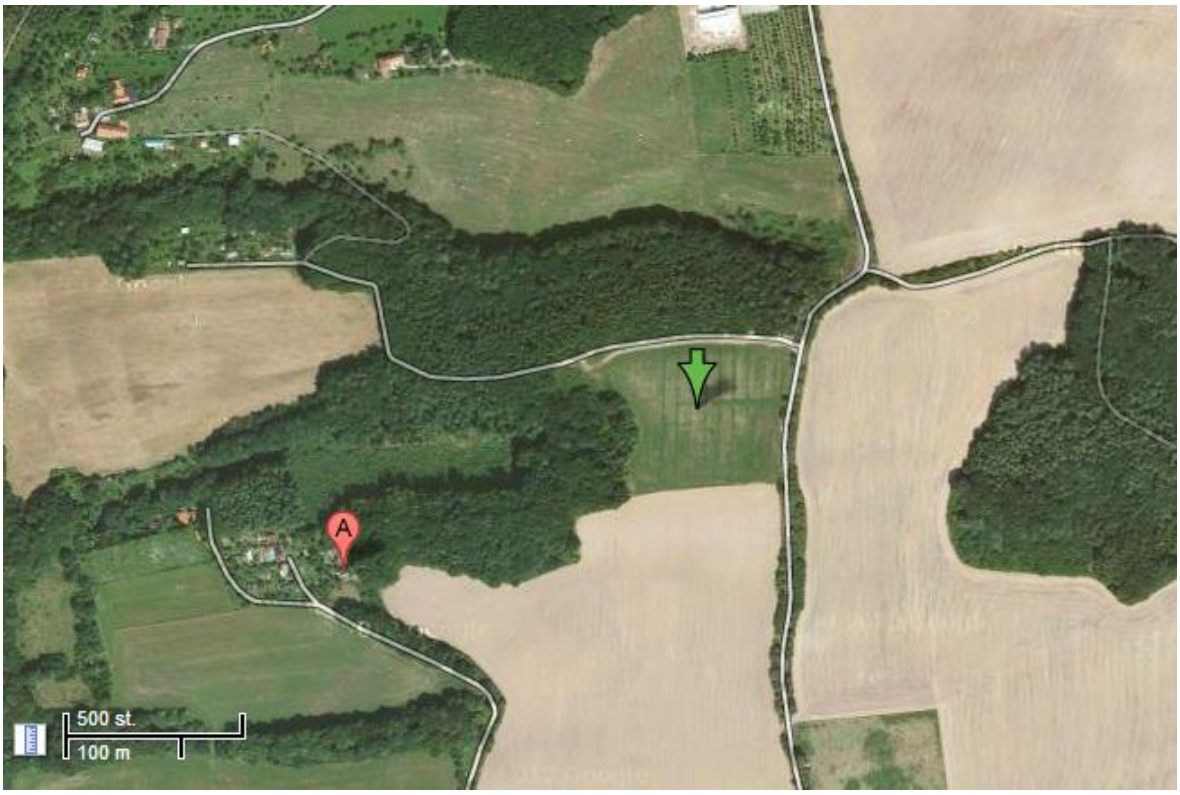
Předmětem bezpečnostní analýzy a návrhu zabezpečení je švestkový sad umístěný na okraji Zlína. Sad je přibližně obdélníkového tvaru o rozměrech 120*170m. Kolem východní strany sadu, ve které je i vstup do areálu (obrázek č. 14) vede asfaltová silnice do další obce. Ze severní strany je tzv. polní cesta, která pokračuje dále do lesa a k chatové oblasti. Areál se rozprostírá celkem přes 3 parcely o celkové rozloze 17829 m^2.



Obrázek 10 Katastrální mapa se zvýrazněným areálem upraveno z [19]

Po provedení bezpečnostní analýzy areálu a přilehlého okolí jsem zjistil v podstatě nulové stávající zabezpečení, areál je ze 3/4 oplocen, zcela chybí oplocení na východní straně (od lesa). Plot je však nízký a nemá žádné bezpečnostní prvky. V místě kde by se měla nacházet vstupní brána je pouze mezera v plotě (obrázek č. 14). Na severní straně se přes ulici nachází rekreační chata patřící jinému majiteli, tudíž se jedná o další bezpečnostní riziko (viz obrázek č. 16).

Na mapce (obrázek č. 11) lze vidět zabezpečovaný areál (zelená šipka) a nejbližší lidské osídlení („A“).



Obrázek 11 Mapka sadu a přilehlého okolí

Na obrázku č. 12 je do mapky zakresleno stávající oplocení červenou barvou a chybějící oplocení barvou bílou. Na východní straně je zaznačena i mezera v plotě, momentálně sloužící pro vstup do areálu. Počítá se však s instalací brány do těchto prostor.

Obrázek 12 Zobrazení stávajícího stavu oplocení

Fotodokumentace stávajícího zabezpečení a rizik.

Obrázek 13 pohled na oplocení ze západní strany (od cesty)

Obrázek 14 Vstup do areálu s chybějící bránou

Obrázek 15 Pohled na rekreační chatu přes severozápadní roh sadu

Obrázek 16 Pohled na rekreační chatu od severní strany oplocení

Obrázek 17 Nedokončené oplocení v severovýchodním rohu

Obrázek 18 Chybějící oplocení východní strany

Obrázek 19 Pohled na jižní stranu

Obrázek 20 Pohled na severní stranu

4.1 Návrh zabezpečení č. 1

Zabezpečení areálu bude provedeno formou, která nebude na první pohled viditelná, tudíž nebude potencionálního pachatele odrazovat, ale bude plně funkční. Areál se obežene novým vyšším oplocením o výšce 2,5m na jehož vrcholu bude navinut ostnatý drát. Dále bude v oplocení navinut odporový drát, který bude snímat otřesy a bude rozdělen na jednotlivé zóny, čímž bude možno zjistit, jestli se jedná o vniknutí pachatele nebo o silný vítr. Ve vzdálenosti 1m za oplocením bude nainstalovaná infrazávora okolo celého areálu ve výšce 50cm. Celý tenhle systém bude připojen do PTZS ústředny, která bude napojena na DPPC najaté externí bezpečnostní agentury. Pro případ příjezdu majitele bude ústředna ovládána dálkovým ovládáním (klíčenkou). Vzhledem k tomu, že jsou v sadu pěstovány pouze trnky, tohle vzdálené připojení bude realizováno pouze po dobu sklizně plodů, srpna a září, z důvodu minimalizace nákladů.

Při hledání infrazávor jsem zvážil nejrůznější možnosti nejvhodnějšího zapojení a 2 závory (6,7) by mohly být s nižším dosahem, ovšem při hledání jsem narazil na závoru od stejného výrobce s dosahem 100m, která byla levnější pouze o 1300kč což se ve výsledku moc neprojeví a nebude tam funkční rezerva pro případné rozšíření, nebo přemístění sadu. Klient je s touto skutečností seznámen a je stejného názoru.

Návrh projektu zabezpečení je vyobrazen na obrázku 21.

Obrázek 21 Návrh 1. varianty

Číslo	Typ	Označení	Cena
1	Pletivo	580m	Cca 70000kč
2	Ostnatý drát	3x250m	Cca 2400kč
3	Vstupní brána		
4	Infrazávora	Optex AX-650DH MKIII	18500kč
5	Infrazávora	Optex AX-650DH MKIII	18500kč
6	Infrazávora	Optex AX-650DH MKIII	18500kč
7	Infrazávora	Optex AX-650DH MKIII	18500kč
8	Infrazávora	Optex AX-650DH MKIII	18500kč
9	Infrazávora	Optex AX-650DH MKIII	18500kč
10	Ústředna	Magellan 5050	2500kč
	Klíčenka	REM 15-433/868	850kč
	Bezpečnostní agentura		300kč/měsíc
		Cena celkem:	186750kč

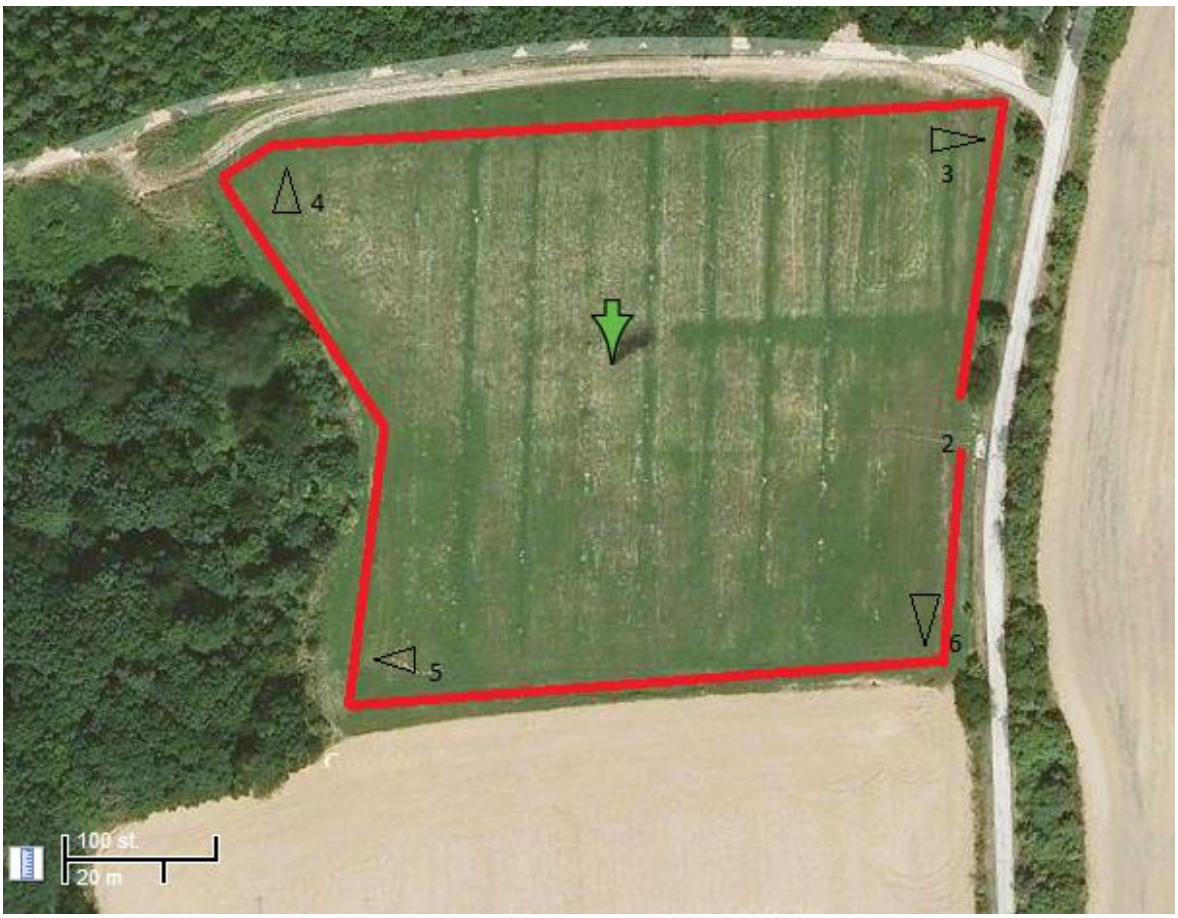
Tabulka 4Cenová kalkulace první varianty

4.2 Návrh zabezpečení č. 2

Původní návrh realizace byl realizován dokončením oplocení, kterým se protáhne odporový drát, rozdělený na zóny. Celý areál bude snímán dvěma termovizními PTZ kamerami v jihozápadním a severovýchodním rohu, které budou rotovat po areálu a reagovat na alarmové vstupy, kdy dojde k zamíření a přiblížení na místo otřesu. Kamery poté vyhodnotí, zda jde o člověka a případně spustí alarm. Celý systém bude napojen na ústřednu aktivovanou dálkovým ovládáním (klíčenkou).

Při průzkumu nabídky na trhu a hledání vhodných kamer jsem narazil na možnost využití kamer bez PTZ za poloviční cenu PTZ. Tudíž bude ušetřena mizivá částka za odporový drát, ale bude velmi ulehčena instalace z důvodu toho, že se kamera nebude muset otáčet na místo, odkud jde poplach, ale máme celý obvod neustále pod kontrolou, takže máme pouze 4 kamery, jejichž alarmový výstup je napojen na ústřednu a v případě rozpoznání člověka dojde ke spuštění alarmu.

Návrh projektu zabezpečení je vyobrazen na obrázku č: 22.



Obrázek 22 Návrh 2. varianty

Číslo	Typ	Označení	Cena
1	Pletivo	580m	Cca 2000kč
2	Vstupní/vjezdová brána		
3	Termovizní kamera	AXIS Q1910-E	80000kč
4	Termovizní kamera	AXIS Q1910-E	80000kč
5	Termovizní kamera	AXIS Q1910-E	80000kč
6	Termovizní kamera	AXIS Q1910-E	80000kč
7	Ústředna	Magellan 5050	2500kč
8	Klíčenka	REM 15-433/868	850kč
		Cena celkem	325350

Tabulka 5 Cenová kalkulace druhé varianty

4.3 Porovnání jednotlivých návrhů

Při porovnání návrhů jsem zjistil docela vysoký cenový rozdíl, cena druhé varianty je téměř dvojnásobná. Je však potřeba vzhledem k umístění a možným výnosům zvážit efektivitu dražší varianty. I u levnější varianty můžeme nainstalovat „falešné“ cedulky o střežení areálu pomocí CCTV systému, což může případného pachatele odradit za minimální cenové navýšení. Výhoda dražšího návrhu je jasná z důvodu možnosti okamžitého zjištění situace ve střeženém areálu. Ovšem i levnější varianta, je efektivně vyřešena, kdy díky dokončení plotu by se přes plot měl dostat pouze pachatel a tudíž by měly být možnost falešných poplachů minimalizována i z důvodu vlastnosti infrazávor, kdy jsou projektovány na venkovní použití, takže ani zhoršené počasí nijak výrazně neomezí jejich funkčnost. Dle mého názoru plně dostačuje první varianta, zvlášť v inkriminovaném období s napojením na DPPC bezpečnostní agentury. Ale realizace bude samozřejmě záležet na přání klienta.

4.4 Popis použitých komponent

4.4.1 Infrazávora Optex AX-650DH MKIII

Obrázek 23 Infrazávora [20]

Vlastnosti:

- Dosah ve venkovním prostředí 200 m.
- Krytí IP65.
- Instalace na sloupek (ø 32 až 48 mm) nebo na rovný povrch.
- Možnost vložení vyhřívací jednotky HU-3.
- Automatická regulace citlivosti.

- Pryžové těsnění zajistí úplnou prachu odolnost a zabrání vniknutí vody.
- Možnost nastavení doby přerušení paprsků 50 / 100 / 250 / 500 ms.
- Přesné nasměrování úzkých, ostře ohraničených paprsků.
- Ochranný kryt se stříškou zabraňuje vzniku námrazy na krytu spodního paprsku.
- Horizontální a vertikální nasměrování paprsků.
- Běžný provoz až do 99% úniku paprsků, tzn., že ani husté sněžení, déšť nebo mlha nesníží funkčnost detektoru.

Technické parametry	
Dosah	200m
Maximální technický dosah	2000m
Detekční metoda	Infračervené paprsky
Doba přerušení paprsků	Volitelně 35,100,250 a 500ms
Napájení	10,5 až 30 V DC
Max. odběr	110mA
Doba sepnutí poplachu	2s (+-1)
Poplachový výstup	22V DC /0,2 A
Tamper	NC sepne při otevření krytu
Vlhkost prostředí	Max 95%
Umístění	Vnitřní/venkovní: na stěnu/na sloupek
Natočení paprsků	+-90° horizontálně, +-20° vertikálně
Pracovní teplota	-35°C až +55°C
Hmotnost	2750g
IP krytí	IP65

Tabulka 6 Technické parametry infrazávory[20]

4.4.2 Termovizní IP kamera AXIS Q1910-E

Obrázek 24Termokamera[21]

Technické parametry	
Provedení kamery	Venkovní IP termovizní kamera
Snímací prvek	Nechlazený Microblometr
Maximální rozlišení	160x128 px
Max. snímková rychlost	8,3 sn/s
Video komprese	H.264, MJPEG
Objektiv	13mm
Detekční dosah	200m člověk, 550m vozidlo
Detekce pohybu	Ano
Poplachový vstup/výstup	2x
Komunikační rozhraní	1x RJ-45 (10/100 Base-t/TX)
Krytí	IP66
Pracovní teplota	-40°C až 50°C
Napájení	8-20V DC / 20-24V AC

Tabulka 7 Technické parametry termovizní kamery[21]

4.4.3 Ústředna Magellan 5050

Obrázek 25 ústředna[22]

Technické parametry	
Podsystémy	2
Max. počet zón	32
Počet vstupů na desce	5 (10 ATZ)
Počet zón na expandérech	24
Historie událostí	256
Napájení	16 V AC
Proudový odběr ústředny	100mA
Firmware	V EEPROM paměti
Max. počet expandérů	3
Bezdrátové zóny	32
Režimy	Úplný, FORCE, STAY, SLEEP
Počet telefonních čísel na PCO	2+1 záložní
Počet telefonních čísel na občanský telefon	5
Pracovní teplota	-10°C až 50°C
Pro stupeň zabezpečení	2. nízké až střední
Klasifikace podle NBÚ	Stupeň utajení 2
Bezdrátové ovládání klíčenkou	Ano

Tabulka 8 Technické parametry ústředny[22]

4.4.4 Klíčenka REM 15-433/868

Obrázek 26 Klíčenka – dálkové ovládání[23]

Technické parametry	
Napájení	Baterie CR 2032
Počet ovládacích tlačítek	4
Frekvence	433/868MHz
Přenos signálu	Technologie plovoucího kódu
Dosah	60m s RTX3 / **45m s MG 5000/MG5050**
Optická signalizace	Červená LED – vysílání
Pro stupeň zabezpečení	2. nízké až střední
Klasifikace podle NBÚ	Stupeň utajení 2

Tabulka 9 Technické parametry dálkového ovládání[23]

5 ODHAD VÝVOJE SYSTÉMŮ DO BUDOUCNA

Vývoj v oblasti bezpečnostních systémů udělal za poslední roky značné kroky kupředu, hlavně díky pokroku v miniaturizaci a elektronice všeobecně. Očekává se i další vývoj do budoucna z důvodu stále více se rozmáhající majetkově trestné činnosti.

Areály sadů zatím dle mých informací těchto možností zabezpečení příliš nevyužívají, ovšem u komerčně orientovaných sadů by se toto řešení mohlo uplatit a předejít tak finančním ztrátám na straně majitele za cenu jedné investice. Hlavní prioritou při zabezpečování sadu je zabezpečit perimetr.

Novinky v tomhle odvětví se budou objevovat jak z oblasti PTZS tak i CCTV, kde očekávám další vývoj v oblasti PZTS a vyšší využití systémů kombinovaných s CCTV z důvodů možných falešných poplachů, ať se již jedná o zvěř anebo přírodní jevy (vítr, déšť, sníh, atd.).

Ohledně vývoje na trhu můžeme spekulovat o snižování cen díky stálé inovace a miniaturizace výroby čipů, kdy se dočkáme zařízení s vyšší efektivitou, nižším odběrem a ztrátovým teplem, což nám umožní odstranit chladicí systémy a minimalizovat velikost celého zařízení.

ZÁVĚR

V bakalářské práci jsem se zabýval základními možnostmi a specifikami zabezpečení areálu sadu, či případně jiného podobného zemědělského areálu.

Každý bezpečnostní systém je prolomitelný. Úkolem bezpečnostních systémů je tedy minimalizovat rizika napadení a vniknutí do zabezpečeného objektu nebo areálu, to znamená několikanásobně prodloužit potřebný časový interval na překonání použitých bezpečnostních prvků a systémů ze strany narušitele, případně narušitele od jeho úmyslu odradit. Při návrhu konkrétního bezpečnostního řešení je potřeba vždy zvážit výhody i nevýhody jednotlivých systémů, s přihlédnutím k finančním možnostem investora.

V teoretické části jsem zpracoval zabezpečení perimetrické ochrany areálu sadu, v jehož rámci lze použít širokou škálu detektorů a CCTV systémů. Perimetrickou ochranu sadu, posuzovaného v praktické části této práce, byla řešena pomocí 2 návrhů, kdy se zatím jedná o realizaci. Podle předběžných propočtů nákladů na základě průzkumu současných cen výrobců, by byla cena druhé varianty téměř dvojnásobná.

Dražší varianta však umožňuje okamžité zjištění situace ve střeženém areálu. Ovšem i levnější varianta, je efektivně vyřešena. Po dokončení plotu by se do areálu měl dostat pouze pachatel a tím pádem by se minimalizovaly falešné poplachy a to i díky vlastnostem infrazávor, které jsou projektovány pro venkovní použití, takže ani zhoršené počasí nijak výrazně neomezí jejich funkčnost. Do jednotlivých návrhů není započítaná cena za kabeláž, vstupní/vjezdovou bránu, napájecí zdroje a práci z důvodu zatím neupřesněné dohody s klientem ohledně provedení.

Klientovi se více zamlouvá druhá varianta, kdy hned po vyhlášení poplachu může zkontrolovat aktuální stav perimetru areálu.

ZÁVĚR V ANGLIČTINĚ

In the thesis I dealt with basic options and specifics of securing the complex of orchard, or possibly other similar agricultural area.

Any security system is to be broken. The task of the security systems is to minimize the exposure to Security threads and penetration into the secure building or campus, it means to extend the time interval required to overcome the security features and systems of the intruder for several times or persuade him from his intetion . When designing a particular security solution is always necessary to consider the advantages and disadvantages of each systems, taking into the financial capacity of the investor.

In the theoretical part, I compiled securing perimeter protection of orchard area, in which we can use a wide range of detectors and CCTV systems. Perimeter protection of orchard, considered in the practical part of this work was solved by two designs, which we are yet dealing about implementing. According to preliminary calculations, the price of second design would almost doubled, based on recoinassance of current prices.

The more expensive design, however allows the immediate determination of the situation in the protected area. But even cheaper option is effectively solved. After completion of the fence would have to get into the area only offender and this would minimize false alarms and also thanks to the properties of the infrared optical barrier, which are designed for outdoor use, so that even worse weather does not significantly restrict their functionality. Designs do not includes the prices of cabling, input / entrance gate, power supplies and work because of yet unspecified agreement with the client.

Client likes more the second option, because after an alarm he can check the current status of the perimeter area.

SEZNAM POUŽITÉ LITERATURY

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

[2] IVANKA, Ján. Mechanické zábranné systémy. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010, 151 s. ISBN 978-80-7318-910-5.

[3] Držák ostnatého drátu. Ploty Wamberk. [online]. 2013 [cit. 2013-05-03]. Dostupné z WWW:http://www.e-pletivo.cz/inshop/ostnate-draty/pictures/store/5_drzak_ostn.jpg

[4] UHLÁŘ, Jan. Technická ochrana objektů II. díl - Elektrické zabezpečovací systémy. Praha : PA ČR, 2001, 208 s. ISBN 80-7251-076-2.

[5] Infrazávora. Express Alarm. [online]. 2013 [cit. 2013-05-03]. Dostupné z WWW:http://www.express-alarm.cz/emdata/products/1362_l.jpg

[6] ČANDÍK, Marek. Objektová bezpečnost. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004, 100 s. Učební texty vysokých škol (Univerzita Tomáše Bati ve Zlíně). ISBN 8073182173.

[7] PIR čidlo. Jablotron. [online]. 2013 [cit. 2013-05-03]. Dostupné z WWW:http://www.jablotron.com/ImageHandler.aspx?method=GetImage&galID=1578&photoID=277986&DontParse=true

[8] Mikrovlnná bariéra. ABBAS. [online]. 2013 [cit. 2013-05-03]. Dostupné z WWW:http://www.abbas.cz/typo3temp/pics/787d7def29.jpg

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

[10] Ústředna. AVC - Systems. [online]. 2013 [cit. 2013-05-03]. Dostupné z WWW:http://www.avc-systems.cz/_websites/ars/soubory/ja-101k.jpg

[11] EUROALARM. Euroalarm. [online]. 2011 [cit. 2013-05-01]. Dostupné z WWW: <http://www.euroalarm.cz/>.

[12] CCTV and Camera Systems. Empire IPS. [online]. 2013 [cit. 2013-05-17]. Dostupné z WWW:http://www.empireips.com/images/CCTV2.jpg

[13] HRUŠKA, F. Technické prostředky automatizace III : Senzory, jejich principy a funkce. Zlín : Univerzita Tomáše Bati ve Zlíně, 2002, 118 s. ISBN 80-7318-053-7.

[14] LAUCKÝ, Vladimír. Technologie komerční bezpečnosti II. Vyd. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007, 123 s. Učební texty vysokých škol (Univerzita Tomáše Bati ve Zlíně). ISBN 978-807-3186-319.

[15] RANDA, Michal. Správa kamerových systémů a zákonem daná informační povinnost.Security Magazín. Praha: Familymedia, 2008, č. 5., s. 38. ISSN1210-8723.

[16] ORWELL, George, 1984, Praha: Levné knihy, 2009, 261s. ISBN 978-80-7309-808-7

[17] BURGESS, Anthony, 1985, Praha: Maťa, 2007, 276s. ISBN 978-80-7287-119-3

[18] Samolepka Tento prostor je monitorován. Tomi Czech Shop. [online]. 2013 [cit. 2013-05-03]. Dostupné z WWW:http://www.t-cz.com/samolepka-tento-prostor-je-monitorovan-kamerovym-systemem-14x10-cm_i7400.jpg

[19] Nahlížení do katastru nemovitostí. Zobrazení katastrální mapy. ČÚZK. [online].2004-2013 [cit. 2013-05-03]. Dostupné z WWW:<http://nahlizenidokn.cuzk.cz/VyberKatastrMapa.aspx#>.

[20] EUROALARM. Infrazávora, 200m - AX-650DH MKIII. Euroalarm. [online]. 2011 [cit. 2013-04-03]. Dostupné z WWW: <http://www.euroalarm.cz/zabezpecovaci-technika/zabezpeceni/detektory/infrazavory/ax-650dh-mkiii>.

[21] KUCHTA, Robert. AXIS Q1910-E - Termovizní IP kamera, 160x128, f=13mm, detekční dosah 200m. Kuchta-elektro. [online]. 2013 [cit. 2013-05-05]. Dostupné z WWW: <http://kuchta-elektro.cz/detail-zbozi/0335-001>.

[22] L.A.S.O.MG-5050, ústředna EZS (2x5=10 zóny ATZ, max.32 zón, 4xPGM). Alarmprovas. [online]. 2013 [cit. 2013-04-05]. Dostupné z WWW:<http://www.alarmprovas.cz/PARADOX%7CEZS/MG%7C5050%7Custredna%7CEZS%7C2x5%7C10%7Czony%7CATZ%7Cmax%7C32%7Czon%7C4xPGM.html>.

[23] L.A.S.O.REM15-433/868, klíčenka (osobní ovladač-vysílač).Almaprovas. [online]. 2013 [cit. 2013-04-03]. Dostupné z WWW:<http://www.alarmprovas.cz/PARADOX%7CEZS/Bezdratove%7Cprvky/REM15%7C433%7C868%7Cklicenka%7Cosobni%7Covladac%7Cvysilac.html>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CCD	Charge - coupled device
CCIR	Comittee Consultatif International Radiotelecommunique
CCTV	Closed Circuit Television
CMOS	Complementary Metal–Oxide–Semiconductor
DPPC	Dohledové a přijímací poplachové centrum
DSP	Digital Signal Processing
GSM	Groupe Spécial Mobile
HDD	Hard Disk Drive
MZS	Mechanické zábranné systémy
PAL	Phase alternating line
PC	Personal computer
PIR	Passive infrared
PIR+MW	Passive infrared + micro wave
PTZ	Pan/Tilt/Zoom
PTZS	Poplachové a tísňové zabezpečovací systémy
RAM	Random Access memory

SEZNAM OBRÁZKŮ

SEZNAM TABULEK