
# VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

## FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

## ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS


# NÁVRH ELEKTRONICKÉHO ZABEZPEČOVACÍHO SYSTÉMU JAKO ČÁST FYZICKÉHO ZABEZPEČENÍ ENERGETICKÝCH OBJEKTŮ KRITICKÉ INFRASTRUKTURY

DIPLOMOVÁ PRÁCE
MASTER'S THESIS


AUTOR PRÁCE
AUTHOR

Bc. Andrej Mihálik

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. Petr Sedlák



BRNO 2018

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

# Zadání diplomové práce

| | |
|---|---|
| Ústav: | Ústav informatiky |
| Student: | **Bc. Andrej Mihálik** |
| Studijní program: | Systémové inženýrství a informatika |
| Studijní obor: | Informační management |
| Vedoucí práce: | **Ing. Petr Sedlák** |
| Akademický rok: | 2017/18 |

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

## Návrh elektronického zabezpečovacího systému jako část fyzického zabezpečení energetických objektů kritické infrastruktury

**Charakteristika problematiky úkolu:**

Úvod a vymezení problému a cíle práce
Teoretické východiska práce
Analýza současného stavu
Návrhová část
Závěr
Přílohy

**Cíle, kterých má být dosaženo:**

Cílem práce je návrh EZS pro energetické objekty prvku kritické infrastruktury.

**Základní literární prameny:**

ČSN ISO/IEC 27001. Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky. Praha: Český normalizační institut, 2014.

ČSN ISO/IEC 27002. Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Soubor postupů. Praha: Český normalizační institut, 2014.

DOUCEK P., V. NOVÁK a V. SVATÁ. Řízení bezpečnosti informací, Praha: Professional Publishing, 2008. ISBN 80-86898-38-5.

ONDRÁK V., P. SEDLÁK a V. MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: CERM, Akademické nakladatelství, 2013. ISBN 978-80-7204-872-4.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2017/18

V Brně dne 28.2.2018

L. S.

| | |
|---|---|
| doc. RNDr. Bedřich Půža, CSc.<br>ředitel | doc. Ing. et Ing. Stanislav Škapa, Ph.D.<br>děkan |

**Abstrakt**

Táto diplomová práca spracúva návrh elektronického zabezpečovacieho systému ako súčasť fyzickej bezpečnosti pre energetickú spoločnosť v Českej republike. Elektronický zabezpečovací systém je navrhnutý tak, aby vyhovel všetkým zákonným požiadavkám, interným smerniciam a obstál aj pri certifikácii podľa normy ISO 27001. Nasadenie zabezpečovacieho systému je modelované na vybranom objekte spoločnosti, ktorý patrí medzi prvky kritickej infraštruktúry.

**Abstract**

This master's thesis deals with the design of an electronic security system as part of the physical security for the energy company in the Czech Republic. The electronic security system is designed to meet all legal requirements, internal directives and has also passed ISO 27001 certification. The Implementation of the security system is demonstrated on the selected object of the company that belongs to the elements of the critical infrastructure.

**Kľúčové slova**

fyzická bezpečnosť, energetická spoločnosť, zabezpečenie, ISMS, kritická infraštruktúra, analýza rizík, poplašný zabezpečovací a tiesňový systém, dohľadový videosystém, elektronická kontrola vstupu

**Key words**

physical security, energy company, security, ISMS, critical infrastructure, risk analysis, alarm security and emergency system, video surveillance system, electronic entry control

**Bibliografická citácia**

MIHÁLIK, A. *Návrh elektronického zabezpečovacího systému jako část fyzického zabezpečení energetických objektů kritické infrastruktury*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2018. 106 s. Vedoucí diplomové práce Ing. Petr Sedlák.

**Čestné prehlásenie**

Prehlasujem, že predložená diplomová práca je pôvodná a spracoval som ju samostatne. Prehlasujem, že citácia použitých prameňov je úplná, že som vo svojej práci neporušil autorské práva (v zmysle Zákona č. 121/2000 Sb., o práve autorskom a o právach súvisiacich s právom autorským).

V Brne, dňa 17. mája 2018

.....

podpis študenta

**Poďakovanie**

Chcel by som poďakovať Ing. Petru Sedlákovi za odborné vedenie diplomovej práce a Ing. Pavlovi Veselkovi za cenné rady pri spracovaní tejto práce. Taktiež ďakujem zamestnancom energetickej spoločnosti za ich ochotu, s ktorou sa podelili o informácie a ich postrehy pri riešení danej problematiky.

# OBSAH

# ÚVOD

Využívanie výpočtovej techniky preniklo do všetkých oblastí dnešnej spoločnosti a podstatne prispieva k zlepšovaniu životnej úrovne populácie po celom svete. Na druhej strane, technologický pokrok vytvára nové možnosti pre ilegálne aktivity. Neustále pribúda počet kybernetických útokov a škodlivého softvéru s cieľom obmedziť poskytované služby, alebo odcudziť citlivé údaje za účelom ich predaja či zneužitia získaných informácií.

Najväčšie riziko predstavuje napadnutie privátnych sietí jednotlivých skupín a organizácií, preto je dôležité pri zvyšovaní informačnej a kybernetickej bezpečnosti dbať aj na zamedzenie akéhokoľvek fyzického prístupu k daným systémom neoprávneným osobám. Jednou zo súčastí informačnej bezpečnosti je aj fyzická bezpečnosť.

Ako už z názvu práce vyplýva, práca sa bude zaoberať návrhom elektronického zabezpečovacieho systému ako súčasť fyzickej bezpečnosti. Práca je rozdelená do 3 kapitol.

**Prvá kapitola** sa zaoberá teoretickými východiskami práce. Vymenováva súvisiace platné zákony a vyhlášky, ktoré musí navrhovaný systém splňovať. Ďalej predstavuje medzinárodné i národné normy, nakoniec sa detailne venuje procesu riadenia rizík.

**Druhá kapitola** analyzuje súčasný stav. Najprv popisuje odvetvie z pohľadu energetiky, následne popisuje legislatívne a regulačné obmedzenia v spomínanom odvetví. Ďalej predstavuje prostredie spoločnosti, pre ktorú je práca spracovávaná. Ďalší bod predstavujú analýzy vonkajšieho i vnútorného prostredia spoločnosti a v závere sú uvedené niektoré riziká súčasného stavu.

**Tretia kapitola** sa zaoberá návrhovou časťou práce. Najprv spracúva technické požiadavky pre elektronický zabezpečovací systém tak, aby splňoval všetky potrebné požiadavky. Nakoniec je nasadenie systému demonštrované na vybranom modelovom objekte.

# VYMEDZENIE PROBLÉMU A CIELE PRÁCE

Hlavným cieľom tejto diplomovej práce je spracovať všeobecný návrh elektronických zabezpečovacích systémov ako časť fyzického zabezpečenia prvkov kritickej infraštruktúry pre energetickú spoločnosť.

Pomocou systému na evidenciu kontroly vstupu bude zaznamenávaný prístup k aktívam spoločnosti, ktoré sú zaradené ako prvky kritickej infraštruktúry podľa krízového zákona jeho vykonávacích predpisov.

Spoločnosť potrebuje tieto systémy jednak preto, aby ako subjekt kritickej infraštruktúry vyhovela legislatívnym požiadavkám na ochranu prvkov kritickej infraštruktúry, taktiež aj preto, aby lepšie chránila svoje aktíva, to znamená majetok ako aj zamestnancov.

Keďže sa jedná o veľkú energetickú spoločnosť, cieľom práce je zjednotiť úroveň zabezpečenia vo všetkých objektoch kritickej infraštruktúry tak, aby vyhovela legislatívnym požiadavkám, normám a interným predpisom spoločnosti.

Vytvorený všeobecný návrh potom bude prakticky nasadený pre jeden modelový objekt, aby sa ukázalo jeho realizovateľné využitie. Podľa tohto pilotného projektu potom bude systém nasadený vo všetkých ostatných objektoch spoločnosti. Musí byť navrhnutý tak, aby ho bolo možné nasadzovať postupne v priebehu času.

# 1 TEORETICKÉ VÝCHODISKÁ PRÁCE

Teoretická časť práce obsahuje teoretické východiská, na ktorých sa zakladajú tvrdenia v analýze súčasného stavu a sú použité ako zdroj znalostnej bázy pri tvorbe vlastných návrhov riešení. Kapitola vysvetľuje pojmy, metódy a postupy použité v ostatných častiach práce.

## 1.1 Základné pojmy a názvoslovie informačnej bezpečnosti

Pre zrozumiteľnosť práce je nutné uviesť základné pojmy a názvoslovie informačnej bezpečnosti, ktoré sú dôležité pre pochopenie spracovávanej problematiky. Ich výklad vychádza z platných noriem rady ČSN ISO / IEC 27000: 2017.

**Aktívum**

Aktívum možno definovať ako všetok hmotný a nehmotný majetok majúci pre vlastníka význam vyjadrený cenou a dôležitosťou, respektíve je použitá kombinácia oboch spôsobov hodnotenia. Vo všeobecnej rovine môže byť aktívom proces, dej, udalosť, ich synchronizácia, a dokonca aj priamo samotný subjekt. Základnými charakteristikami každého aktíva sú jeho hodnota a zraniteľnosť. (2, 5)

**Dáta**

Dáta sú nositeľmi zaznamenaných skutočností a vytvárajú opakovane interpretovateľnú a oficiálnu podobu informácie, ktorá je vhodná pre komunikáciu, vyhodnocovanie, alebo pre potreby následného spracovania. (5)

**Informácie**

Informácie popisujú reálne prostredie, jeho stav a procesy v ňom prebiehajúce vo forme údajov, pričom jej rastúce množstvo znižuje mieru entropie pred a po prijatí správy. V reálnom svete sa daná informácia vyskytuje v rôznych formách, môže byť vytlačená, alebo napísaná na papieri, ukladaná v elektronickej podobe, posielaná poštou, alebo elektronickou cestou, či vyslovená pri konverzácii. V odbore informatiky vystupuje v

podobe kódovaných dát prostredníctvom fyzikálnej interpretácie v úložnom zariadení, alebo na prenosovom médiu. Informácie pre organizácie všetkých druhov a veľkostí predstavujú **významné aktívum**, čím vzniká požiadavka na ich primeranú ochranu. Informačné a komunikačné technológie predstavujú dôležitý nástroj nielen pre ich vytváranie, spracovanie, ukladanie a prenos, ale aj **zabezpečenie.** (2, 5)

**Informačný systém**

Z dôvodu rôznorodosti terminológie neexistuje presná definícia informačného systému, avšak možno ho chápať ako sústavu vzájomne prepojených informácií a procesov, ktoré s týmito informáciami pracujú. (5)

**Dostupnosť**

Dostupnosť predstavuje zabezpečenie prístupnosti a použiteľnosti informácie len oprávnenému užívateľovi v požadovaný okamih. (2)

**Dôvernosť**

Dôvernosť je vlastnosť, ktorá zaručuje prístup alebo poskytnutie informácie výhradne oprávnenej osobe, entite, alebo postupu. (2)

**Integrita**

Pojem integrita vymedzuje správnosť a úplnosť informácie, ktorú nie je možné modifikovať alebo poškodiť pri neautorizovanom prístupe. (2)

**Zraniteľnosť**

Pod zraniteľnosťou sa rozumie slabé miesto aktíva, alebo opatrenie, ktoré môže byť zneužité jednou, alebo viacerými hrozbami. (2)

**Hrozba**

Hrozba označuje potenciálnu príčinu nežiaduceho incidentu, ktorý vzniká zneužitím zraniteľnosti aktíva a môže mať za následok poškodenie systému, alebo organizácie. Hlavnou charakteristikou hrozby je jej úroveň, ktorá je zvyčajne klasifikovaná na

základe schopnosti spôsobiť škodu, možnosti pôsobenia na aktívum, alebo záujmu o naplnenie hrozby. Dopad hrozby vymedzuje vznik škody v dôsledku pôsobenia hrozby. (1)

**Incident**

Incident je nežiaduca, alebo neočakávaná udalosť, ktorá môže s veľkou pravdepodobnosťou vyvolať ohrozenia bezpečnosti informácií. (2)

**Opatrenie**

Opatrenie je: postup, proces, fyzický prostriedok, služba, či čokoľvek, čo bolo navrhnuté a je určené pre zmiernenie, alebo úplné vylúčenie zraniteľnosti, dopadu, či pôsobenia hrozby. Jeho rozsah predstavuje úroveň opatrení a podľa typu sa členia na preventívne, podporné, detekčné a reaktívne. Miera plnenia účelu v reálnom procese sa označuje ako účinnosť opatrení. (2)

**Riziko**

Riziko vzniká pôsobením hrozby na aktíva a vyjadruje mieru ich ohrozenia. Predstavuje odlišný a nežiaduci vývoj od predpokladaného s nebezpečenstvom vzniku škody, poškodenia, straty či zničenia. Riziko vytvára stav neistoty, ktorý sa spravidla vyjadruje pomocou pravdepodobnosti v rozmedzí hodnôt 0 a 1. Existencia rizika súvisí s neurčitosťou výsledku, pričom v množine variant vývoja sa vyskytuje aspoň jeden nežiaduci variant. (1, 2)

**Bezpečnostná udalosť**

Bezpečnostnú udalosť určuje identifikovaný stav systému, služby alebo siete, ktorá poukazujúce na možnosť porušenia bezpečnostnej politiky, alebo zlyhania bezpečnostných opatrení. Môže sa jednať aj o inú, predtým neuskutočnenú, situáciu, ktorá je dôležitá z pohľadu bezpečnosti informácií. (3)

**Bezpečnostný incident**

Pojem bezpečnostný incident predstavuje jednu, alebo viacero nežiaducich bezpečnostných udalostí, pri ktorých existuje vysoká pravdepodobnosť kompromitácie činnosti organizácie a ohrozenie bezpečnosti. (3)

**Bezpečnosť informácií**

Bezpečnosť informácií je tvorená tromi hlavnými dimenziami, ktorými sú **dôvernosť**, **dostupnosť** a **integrita**. Zahŕňa implementáciu a správu bezpečnostných opatrení, zameraných na širokú škálu hrozieb a zaisťuje tak zmierňovanie dopadov bezpečnostných incidentov, kontinuitu činností organizácie. Minimalizuje obchodné straty a maximalizuje návratnosť investícií a podnikateľských príležitostí. Informačnej bezpečnosti je dosiahnuté pri vykonávaní súboru kontrol, vybraných v rámci procesu riadenia rizík a spravovaných pomocou ISMS, vrátane politík, procesov, postupov, softvéru a hardvéru pre ochranu informačných aktív. (5)

Informačná bezpečnosť je úzko prepojená s pojmami **bezpečnosť organizácie** a **bezpečnosť IS/ICT**. Bezpečnosť organizácie, ktorej zámerom je ochrana majetku spoločnosti, je prikladaná najvyššia priorita a obsahuje bezpečnosť IS/ICT a bezpečnosť informácií. Bezpečnosť informácií obsahuje bezpečnosť IS/ICT a prácu s informáciami v nedigitálnej forme. Bezpečnosť IS/ICT chráni len aktíva informačného systému podporovaná informačnými a komunikačnými technológiami. (5)

## 1.2 Systém riadenia bezpečnosti informácií

Systém riadenia bezpečnosti informácií - ISMS (Information Security Management System) je efektívny, dokumentovaný systém riadenia a správy informačných aktív, s cieľom eliminovať ich možnú stratu, alebo poškodenie. V prvom rade sú určené aktíva, ktoré sa majú chrániť, potom sú vybrané a riadené možné riziká bezpečnosti informácií a zavedené opatrenia s požadovanou úrovňou záruk a v poslednom rade kontrola. Z dôvodu zaistenia dostatočnej efektivity bezpečnosti informácií musí ísť o riadený proces vyvážený vo všetkých oblastiach, ktorý má podporu vedenia a rešpektuje

kultúru organizácie. Ekonomické hľadisko ISMS vyžaduje dosiahnutie informačnej bezpečnosti za akceptovateľné náklady. (3, 5, 6)

ISMS tvorí časť celkového systému riadenia organizácie, založeného na prístupe k rizikám činnosťou, ktorá je zameraná na stanovenie, zavádzanie, prevádzku, monitorovanie, preskúmanie, udržiavanie a zlepšovanie bezpečnosti informácií. ISMS zahŕňa organizačnú štruktúru, politiky, plánovacie činnosti, zodpovednosti, praktiky, postupy, procesy a zdroje. Rozsah zavedenia systému riadenia bezpečnosti informácií je strategickým rozhodnutím spoločnosti a môže obsahovať **organizačnú zložku**, **informačný systém** alebo jeho časť, **prípadne celú organizáciu**. Na všetky procesy v ISMS možno aplikovať model PDCA. (5)

### 1.2.1 Model PDCA

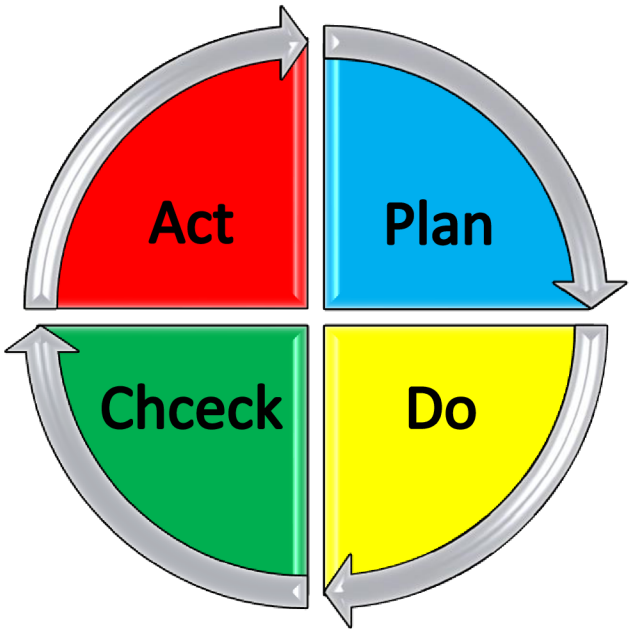
Model PDCA, tiež známy ako Demingov cyklus, ktorý predstavuje druh iteratívnej metódy postupného zlepšovania formou opakovaného vykonávania zmien v štyroch etapách, ktorými sú:

- **Plan (plánuj)** - naplánovanie zamýšľaného zlepšenia,
- **Do (rob)** - realizácia plánu,
- **Check (kontroluj)** - overenie výsledku realizácie oproti pôvodnému zámeru,
- **Act (konaj)** - úpravy zámeru a implementácia zlepšení do praxe. (1, 5)

Systém riadenia bezpečnosti informácií je založený na využití PDCA cyklu, ktorý býva označovaný ako životný cyklus ISMS, ktorého jednotlivé fázy tvorí:

- **Zriadenie ISMS** - určenie rozsahu a zodpovednosti, kde patria časti ako: preskúmanie ISMS, rozsah ISMS, politika ISMS, správa o hodnotení rizika, súhlas so zavádzaním ISMS, vyhlásenie o aplikovateľnosti.
- **Zavádzanie a prevádzka ISMS** - presadenie vybraných bezpečnostných opatrení, ako napríklad plán zvládania rizík, príručka bezpečnosti informácií, program bezpečnostného povedomia, indikátory a metriky bezpečnosti, riadenia zdrojov, dokumentov a záznamov.

- **Monitorovanie a preskúmanie ISMS** - zabezpečenie spätnej väzby a hodnotenia riadenia. Vyhodnotenie incidentov monitorovania a kontroly, merania účinnosti ISMS, plán interných auditov ISMS, správa o stave ISMS.
- **Údržba a zlepšovanie** - odstraňovanie slabín a sústavné zlepšovanie, zlepšovanie ISMS, opatrenia na nápravu ISMS, preventívne opatrenia ISMS. (1, 5)




Obrázok 1: PDCA cyklus (vlastné spracovanie)

### 1.2.2 Rad noriem ISMS

Pred uvedením najdôležitejších noriem zaoberajúcich sa problematikou ISMS je vysvetlený rozdiel medzi pojmami **štandard** a **norma**. Taktiež sú predstavené niektoré normalizačné inštitúcie, zaoberajúce sa štandardizáciou bezpečnosti informačných technológií na rôznych úrovniach. (2, 5)

#### Štandard

Štandard predstavuje zdokumentovanú dohodu obsahujúcu **technické špecifikácie,** alebo **presne** stanovené **kritériá,** dôsledne používané ako striktné pravidlá. Štandard môže slúžiť ako definícia charakteristických vlastností, ktoré zabezpečia požadovanú kvalitu materiálu, výrobku, procesu a služby. (4, 5)

**Norma**

Norma je **odporúčanie** pre daný štandard **k realizácii** požadovaného kompatibilného riešenia. Kým normy sú veľmi často výsledkom ťažko dosiahnutého kompromisu, štandardy bývajú zdrojom k dynamickému presadeniu technickej politiky a následného pokroku. (5)

**ISO**

Poslaním medzinárodnej organizácie ISO je podporovanie rozvoja štandardizačných a s tým spojených aktivít, zameraných na uľahčenie medzinárodných smien tovaru a služieb, tiež na spoluprácu vo sfére: intelektuálnej, vedeckej, technologickej a ekonomickej. (5)

**IEC**

Organizácia IEC pripravuje a vydáva medzinárodné normy z oblasti elektrotechnických, elektronických a im príbuzných odboroch. (5)

**NIST**

Národný inštitút pre normy a technológie (The National Institute of Standards and Technology) je súčasťou amerického ministerstva obchodu. NIST je jedným z národných laboratórií fyzikálnych vied, kde merajú produkty a služby, následne vydávajú štandardy. Jednou z oblastí merania a štandardizácie je práve **kybernetická bezpečnosť**. (5)

**ČSN**

Česká technická norma (ČSN) vzniká dvojakým spôsobom. Do sústavy českých technických noriem sa **harmonizujú** európske a medzinárodné normy formou ČSN EN, alebo sú vytvorené **pôvodné** ČSN, vyplývajúce z národných potrieb a hľadísk na zachovanie funkčnosti fondu ČSN. (4 ,5)

### Rad noriem ISMS

Rad noriem ISMS obsahuje zoznam medzinárodných noriem, ktoré majú spoločný názov **Informačné technológie - Bezpečnostné techniky**. Skladá sa zo vzájomne súvisiacich noriem, ktoré obsahujú významné štrukturálne komponenty, zameriavajúce sa na technické normy, popisujúce požiadavky na ISMS (ISO/IEC 27001). Tiež aj na organizácie certifikujúce zhodu s ISO/IEC 27001 (ISO/IEC 27006). Ďalšie technické normy poskytujú návod pre rôzne stránky implementácie ISMS a zaoberajú sa všeobecnými smernicami vo vzťahu k opatreniam, či špecifickými návodmi, delených podľa odvetví (2).

### Zoznam noriem rady ISMS

Nasledujúca tabuľka č. 1 popisuje prehľad noriem ISMS. Normy sú zoradené podľa číselného pridelenia. Obsahujú popis danej normy a kategóriu, do ktorej patria.

Tabuľka 1: Zoznam noriem rady ISMS (vlastné spracovanie, 2)

| | | |
|---|---|---|
| **Norma obsahujúca terminológiu** | 27000 | Prehľad a slovník |
| **Normy špecifikujúce požiadavky** | 27001 | Systém riadenia bezpečnosti informácií - Požiadavky |
| | 27006 | Požiadavky na orgány poskytujúce audit a certifikáciu systémov riadenia bezpečnosti informácií |
| **Normy popisujúce všeobecne smernice** | 27002 | Súbor postupov pre opatrenia bezpečnosti informácií |
| | 27003 | Smernica pre implementáciu systémov riadenia bezpečnosti informácií |
| | 27004 | Riadenie bezpečnosti informácií - Meranie |
| | 27005 | Riadenie rizík bezpečnosti informácií |
| | 27007 | Smernica pre audit systémov riadenia bezpečnosti informácií |
| | 27008 | Smernica pre audit opatrení ISMS |
| | 27013 | Návod pre integrovanú implementácii ISO / IEC 27001 a ISO / IEC 20000-1 |
| | 27014 | Správa bezpečnosti informácií |
| | 27016 | Riadenie bezpečnosti informácií - Organizačná ekonomika |
| **Normy popisujúce smernice špecifické pre odvetvie** | 27010 | Smernica riadenia bezpečnosti informácií pre medzisektorovú komunikáciu a komunikáciu medzi organizáciami |

| | | |
|---|---|---|
| | 27011 | Smernice pre riadenie bezpečnosti informácií telekomunikačnej organizácie na základe ISO / IEC 27002 |
| | 27015 | Smernice pre riadenie bezpečnosti informácií pre finančné služby |
| | 27017 | Smernice pre opatrenia bezpečnosti informácií pri použití služieb cloud computingu na základe ISO / IEC 27002 |
| **Ostatné normy popisujúce smernice špecifické pre opatrenia** | 2703x , 2704x | |

## 1.3 Predbežná norma ČSN P 73 4450-1

Predbežná česká štátna norma 73 4450-1 stanovuje všeobecné požiadavky na systém fyzickej ochrany prvkov kritickej infraštruktúry pre minimalizáciu dopadov antropogénnych hrozieb, vrátane teroristického útoku. Je určená predovšetkým pre subjekty kritickej infraštruktúry v odvetví energetiky. Ostatným užívateľom môže slúžiť ako metodický návod pre nadobudnutie úrovne bezpečnosti a rozsahu fyzickej ochrany prvkov kritickej infraštruktúry. (6)

Norma rozdeľuje bezpečnostné opatrenia fyzickej ochrany na **technické**, **režimové opatrenia** a **fyzickú ochranu.** Významný podiel na zaistení účinnej a efektívnej úrovne fyzickej ochrany má kategorizácia objektov a bezpečnostné zónovanie objektov. Bezpečnostné zónovanie objektov je nevyhnutnou súčasťou kategorizácie objektov. Samotné zónovanie definuje a spresňuje jednotlivé opatrenia v rámci objektu. (6)

Technické opatrenia, ktorými norma rozumie mechanické a elektronické prostriedky, ktoré majú za úlohu chrániť hranicu areálu, plášť objektu a vnútorné priestory objektu, sa potom ďalej delia na **elektrickú požiarnu signalizáciu** a **systém technickej ochrany**, u ktorých vymenováva jednotlivé prvky. (6)

Režimovými opatreniami sa rozumie súbor interných záväzných a presne definovaných pokynov, príkazov obmedzení a postupov, zaisťujúci vzájomné väzby medzi bezpečnostnými opatreniami a užívateľmi objektu. (6)

Norma definuje požiadavky na osoby poverené výkonom fyzickej ochrany a vymenováva činnosti, ktoré by tieto osoby mali vykonávať. (6)

### 1.3.1 Bezpečnostné kategórie objektov

Tabuľka 2: Bezpečnostné kategórie objektov (vlastné spracovanie, 6)

| Kategória | Všeobecná charakteristika objektu | Príklad |
|---|---|---|
| **I.** | Objekty v súlade s vyhláškou č. 361/2016 Sb., o zabezpečenie jadrových zariadení a jadrových materiálov | Nedefinované |
| **II.** | **Prvok KI alebo objekt s kritickým významom pre prvok KI.**<br>Objekt nenahraditeľný, alebo ťažko nahraditeľný.<br>Objekt má kritický význam pre fungovanie a riadenie dodávok elektrickej energie. | - Technický dispečing prevádzkovateľa.<br>- Elektrická stanica prenosovej sústavy s napätím najmenej 110 kV.<br>- Elektrická stanica distribučnej sústavy.<br>- Záložný dispečing prevádzkovateľa prenosovej a distribučnej sústavy.<br>- Priestory s dislokáciou prvkov kritickej informačnej infraštruktúry<br>- Dohľadové a prijímacie poplachové centrum DPPC, dohľadový dispečing.<br>-Priestor s pracoviskom krízového štábu podľa zákona č. 240/2000 alebo zabezpečenej oblasti podľa zákona č. 412/2005 Sb. |
| **III.** | **Objekt sa zásadným významom pre prvok KI.**<br>Objekt ťažko nahraditeľný pre funkčnosť systému.<br>Poškodenie, či vyradenie, má závažný vplyv na funkčnosť dotknutej časti systému dodávok elektrickej energie.<br>V prípade vyradenia niektorého z objektov dôjde ku komplikáciám prípadne k nedodaniu elektrickej energie v danom územnom celku. | – Elektrická stanica distribučnej sústavy vvn / vn (220 kV; 110 kV / 22 kV),<br>– Spínacia stanica vvn (220 kV; 110 kV),<br>– Administratívne centrá charakteru sídla spoločnosti. |
| **IV.** | **Objekt s dôležitým významom pre zabezpečenie funkčnosti prvku KI.**<br>Objekt podporného charakteru na zabezpečenie činnosti objektov kat. II a III.<br>Vyradením objektu dôjde k nezanedbateľným komplikáciám, prípadne k nedodaniu elektrickej energie v danej lokalite | – Elektrická stanica distribučnej sústavy vn / vn (3; 6; 10; 22; 35 kV).<br>– Spínacia stanica vn (3; 6; 10; 22; 35 kV),<br>– Záložné zdroje elektrickej energie,<br>– Zdroje médií (voda, teplo),<br>– Ostatné chránené a administratívne objekty a prevádzkové centrá. |
| **V.** | **Objekty s malým významom pre zabezpečenie funkčnosti prvku KI.**<br>Objekty s malým významom pre zabezpečenie funkčnosti prvku KI.<br>Objekt podporného charakteru na zabezpečenie činnosti objektov kategórie II až IV. | – Distribučná transformačná stanica vn/nn. |
| **Objekty bez kategórie** | Objekt, ktorého poškodenie, či vyradenie, nemá žiadny priamy vplyv na funkčnosť dodávok elektrickej energie.<br>**Objekt využívaný podpornými službami na zabezpečenie, alebo obnovenie prevádzkyschopnosti prvku.** | – Sklady,<br>– Dielne,<br>– Garáže. |

### 1.3.2 Bezpečnostné zónovanie objektov

Pod pojmom bezpečnostné zónovanie sa chápe stavebne vymedzená časť podľa kategorizovaného objektu, v ktorej sú dislokované časť prvkov KI (napr. Technická miestnosť s prvkami kritickej informačnej infraštruktúry v priestoroch elektrickej stanici). Bezpečnostnou zónou sú tak vymedzené významné časti prvkov KI pre zaistenie procesov prenosu a distribúcie elektrickej energie. (6)

Jednotlivé zóny (priestory) sú tvorené vymedzenou časťou pozemku, stavebným objektom alebo súborom miestností, ktoré sú spravidla vzájomne oddelené. Tie musia byť zaradené do príslušných bezpečnostných zón, ktoré sú uvedené v tabuľke č. 3.

Tabuľka 3: Bezpečnostné zónovanie objektov (vlastné spracovanie, 6)

| Kategória | Bezpečnostná zóna | Charakteristika zóny | Príklad |
|---|---|---|---|
| **A** | zvlášť zabezpečená | **Zvlášť chránený priestor s kritickým významom pre funkčnosť systému dodávok elektrickej energie.** Ide o striktne režimovo vymedzené priestory, ktoré musia byť dislokované len v objekte kategórie II a III. | – technický dispečing,<br>– dohľadové centrá,<br>– pracovisko ICT<br>– serverovňa |
| **B** | zabezpečená | **Priestor so zvýšenou ochranou so zásadným významom pre funkčnosť systému dodávok elektrickej energie, vrátane následnej distribúcie koncovým užívateľom.** Jedná sa o ohraničené priestory, ktoré musia byť dislokované v objekte kategórie II až IV. | – riadiacej jednotky poplachových a prenosových systémov,<br>– záznamové zariadenie VSS,<br>– rozvádzače prenosov. |
| **C** | chránená | **Priestor s dôležitým významom pre bezpečnosť dodávok elektrickej energie.** Priestor, kde sú umiestnené komponenty, ktoré svojím významom majú vplyv na zabezpečenie funkcií objektov KI | – vybrané skladové priestory,<br>– priestory, kde sú umiestnené generátory, TVS,<br>– miestny velín,<br>– telefónna ústredňa. |
| **D** | kontrolovaná | **Kontrolovaný priestor podporných pracovísk dodávok elektrickej energie** Pracovisko nemá priamy význam pre bezpečnosť dodávok elektrickej energie, ale ich vyradenie by mohlo určitým spôsobom ohroziť tento proces | – vybrané odstavné a manipulační plochy,<br>– ostatné vonkajšie plochy či priestory vymedzenej vonkajším perimetrom objektu (areálu),<br>– vybrané dielenské priestory dielne. |

Na stanovenie konkrétnej bezpečnostnej zóny má zásadný vplyv možnosť fyzického vymedzenia jej hranice. Pri stanovení bezpečnostnej zóny môžu nastať situácie, kedy v

objekte určitej bezpečnostnej kategórie je dislokovaný stavebný objekt, alebo priestor tvorený inou kategóriou bezpečnostnej zóny. Spoločné vonkajšie hranice (perimetre) objektu a hranica bezpečnostnej zóny môžu byť chránené (6):

a) totožné (podľa perimetra objektu) - v prípade, keď požiadavky na perimeter objektu sú vyššie ako na hranicu bezpečnostnej zóny,
b) odlišné (v časti bezpečnostnej zóny) - v prípade, že je vo vnútri objektu bezpečnostná zóna významovo vyššie, aplikuje sa štandard pre hranicu bezpečnostnej zóny. (6)

### 1.3.3 Technické opatrenia

Technické bezpečnostné opatrenia znamenajú mechanické a elektronické prostriedky ochrany, ktoré majú za úlohu chrániť hranicu (perimeter) objektu, alebo plášť bezpečnostnej zóny (prostriedky vonkajšej ochrany), ale aj ich vnútorné priestory (prostriedky vnútornej ochrany). (6)

**Systém technickej ochrany**

Medzi technické oparenia podľa ČSN P 73 4450-1 patrí systém technickej ochrany (STO) a požiarna signalizácia. Je to súbor prostriedkov vnútornej a vonkajšej ochrany, ktorý zabraňuje, sťažuje, detekuje a dokumentuje narušenie fyzickej ochrany prvkov KI. Systém technickej ochrany objektov tvoria najmä:

a) mechanické zábranné prostriedky (MZP),
b) poplachové elektronické systémy:
   - poplachový zabezpečovací a tiesňový systém (PZTS),
   - dohľadové videosystémy (VSS),
   - elektronické systémy kontroly vstupu (EKV),
   - poplachové prenosové systémy a zariadenia,
   - kombinované a integrované systémy,
c) dohľadové a prijímacie poplachová centrá (DPPC),
d) špeciálne systémy,

e) núdzové zvukové systémy a hlasové výstražné zariadenie,

f) bezpečnostné a núdzové osvetlenie. (6)

**Mechanické zábranné prostriedky**

Mechanické zábranné prostriedky slúžia na zamedzenie prístupu, alebo jeho sťaženie, prípadne k odradeniu náhodného páchateľa pred vniknutím do chráneného priestoru. Zároveň vytvára časový odstup pre prijatie vhodných opatrení proti narušiteľovi (detekcia pokusu o narušenie objektu). (6)

Jednotlivé prostriedky sú:

- oplotenia a ohradenia,
- dvere, brány, vráta, turnikety, okná, mreže, okenice,
- bezpečnostné sklá a fólie,
- zámky a uzamykacie systémy. (6)

Mechanické zábranné prostriedky možno rozdeliť i podľa oblasti ich využitia:

Perimeter areálu

- vonkajšie oplotenie,
- vstupy (vstupná brána) a vjazdy (vjazdová a vlečkové brána),
- budovy v perimetri. (6)

Vonkajšie priestory

- vonkajšie stanovištia silového energetického zariadenia,
- odstavné plochy vo vnútri objektu s uloženým majetkom,
- vstupy do priechodných káblových kanálov. (6)

Vnútorné priestory a budovy

- vstupné dvere a brány v plášti budovy, vrátane núdzových východov a vstupov z káblových kanálov,

- uzamykací systém, alebo visiaci zámok vo vstupných dverách a vrátach do budovy,
- samozatvárací mechanizmus na hlavných vstupných dverách do budovy,
- presklené časti v plášti budovy (dvere, okná),
- presklené časti v plášti budovy pod úrovňou okolitého terénu (pivničné okná),
- ďalšie technické otvory v plášti budovy,
- pevné rebríky na plášti budovy ústiace na strechu. (6)

**Poplachový zabezpečovací a tiesňový systém**

Poplachový zabezpečovací systém (PZTS) slúži k včasnému detekovaniu, indikácii a vyhodnocovaniu neoprávneného vniknutia či napadnutia osôb, vyrozumeniu zásahových skupín a fyzickej ochrany, či aktiváciu ďalších bezpečnostných opatrení. Mimo to môže slúžiť aj ako nástroj na kontrolu dodržiavania režimových opatrení. (6, 7)

Najdôležitejším prvkom v PZTS je ústredňa, ktorá celý systém koordinuje. Prijíma dáta od pripojených senzorov, ktoré vyhodnocuje na základe programu v pamäti ústredne. K ústredni sú pripojené aj signalizátory poplachu, ako napríklad: sirény, výstražné majáky, GSM moduly na posielanie správ. Typ ústredne určuje maximálny možný počet pripojených modulov. Na základe komunikácií s ostatnými modulmi ústredne sa rozdeľujú na slučkové, zbernicové a bezdrôtové. (6, 7)

Ochrana perimetra slúži na signalizáciu prítomnosti prípadného narušiteľa na hranici areálu, teda ešte predtým, než sa priestorom areálu priblíži ku stráženým objektom. Vďaka tejto ochrane je možné detekovať zmeny na oplotení pri jeho narušení, ako sú vibrácie, mechanické poškodenia a iné. Tiež chráni rizikové časti (vyhodnotené bezpečnostným posúdením), signalizáciu otvorenia využívaných vstupov a vjazdov do perimetra. (6)

Ochrana priestoru a plášťa budovy je určená predovšetkým na včasnú detekciu prítomnosti alebo pokusu o neoprávnené vniknutie narušiteľa do **stráženého priestoru**, ochrane predmetov a privolanie pomoci v prípade tiesne. Je zároveň určený na signalizáciu poplachových stavov do miesta s trvalou strážnou službou. (6)

Tiesňové systémy signalizuje ohrozenie života, alebo zdravotné problémy fyzických osôb, ktoré sú napadnuté, ohrozené pôsobením prírodných živlov (požiar, voda, plyn), alebo vystavené mimoriadnej udalosti, pri ktorej je nutné patrične reagovať (teroristický útok). Signalizácia je vyvolaná manuálne (stlačenie tlačidla), definovaným spôsobom manipulácie (nášľapná tiesňová lišta), alebo automaticky. (6)

**CCTV sledovacie systémy**

CCTV systémy sa používajú na sledovanie, prenos, zobrazovanie a dokumentáciu pohybu osôb a dopravných prostriedkov. Poskytujú rýchle a spoľahlivé obrazové informácie pre zabezpečovacie, bezpečnostné a monitorovacie činnosti. Ich záznam možno spätne vyhodnocovať. Umožňujú diaľkový dohľad v prípade neprítomnosti osôb v objekte :

- pevné a otočné kamery,
- špeciálne kamery (napr. termovízne). (6, 9)

**Elektronické systémy kontroly vstupu**

Systém kontroly vstupu zabezpečuje režim vstupu osôb a vjazdu dopravných prostriedkov do chránených priestorov. Pomocou neho možno kontrolovať a dokumentovať pohyb v chránených priestoroch podľa nastavených oprávnení, teda aj identifikovať pokusy o neoprávnený prístup do chránených priestorov. Medzi prostriedky pre zabezpečenie EKV sa môžu používať napríklad:

- čipy,
- identifikačné karty,
- biometrické snímače. (6, 10)

**Poplachové prenosové systémy a zariadenia**

Poplachové prenosové systémy pomocou prenosových prostriedkov prenášajú informácie zo zabezpečovacích zariadení. (6)

**Kombinované a integrované systémy**

Kombinované a integrované systémy automatizujú vzájomné väzby jednotlivých systémov, čím zjednodušujú ich obsluhu. Vzájomne integrované systémy si medzi sebou môžu vymieňať informácie, zdieľať niektoré zariadenia, ich vybavenie a prenosové trasy. Môžu byť schopné poskytovať doplnkové informácie (obrazom, textom, alebo zvukom). (6, 10)

**Dohľadové a poplachové príjmové centrá**

Dohľadové centrá vykonávajú nepretržitý dohľad nad pripojenými poplachovými systémami. Včas zisťujú, indikujú a vyhodnocujú všetky poplachové i poruchové signály. Závisí na nich rýchlosť a efektívnosť zákroku zásahových skupín a fyzickej ochrany. (6)

**Núdzové zvukové systémy a hlasové výstražné zariadenia**

Núdzové zvukové systémy majú za cieľ vysielať informácie a prípadne riadiť evakuáciu. Používajú sa systémy s tónovými signálmi (napr. siréna, klaksón) a systémy s hlasovým hlásením (napr. obecný rozhlas). (6)

**Bezpečnostné a núdzové osvetlenie**

Bezpečnostné a núdzové osvetlenie si kladie za cieľ odradenie náhodného páchateľa pred vniknutím do chráneného priestoru, prípadne jeho ľahšiu identifikáciu. (6)

Príklad technických prostriedkov:

- trvalé osvetlenie za zníženej viditeľnosti,
- osvetlenie pri detekcii pohybu. (6)

**Elektrická požiarna signalizácia**

Požiarna signalizácia je často súčasťou kombinovaných a integrovaných systémov. Inštaluje sa v súlade s požiadavkami danými príslušnými právnymi predpismi o požiarnej ochrane, o požiarnej prevencii a o technických podmienkach požiarnej ochrany. EPS musí byť inštalované pri prvkoch KI v objektoch bezpečnostnej kategórie

I., odporúča sa však inštalácia aj v ďalších dôležitých objektoch. V objektoch prvku KI, kde nie je vyžadovaná inštalácia EPS, možno zabezpečiť signalizáciu vzniku požiaru snímačmi zapojenými do PZTS. (6)

### 1.3.4 Režimové opatrenia

Režimovými opatreniami je súbor interných, písomne definovaných pokynov, príkazov, obmedzení a postupov, slúžiacich na stanovenie režimu a spôsobu použitia bezpečnostných opatrení. Režimové opatrenia sa týkajú všetkých osôb, ktoré vstupujú (vchádzajú) alebo vychádzajú (odchádzajú) a pohybujú sa v objekte, či bezpečnostnej zóne. (6)

Medzi režimové opatrenia patria najmä:

- režim vstupu / výstupu osôb (pracovníci, pracovníci tretích strán, návštevy),
- režim vjazdu / výjazdu motorových vozidiel,
- režim pohybu osôb a vozidiel v objekte,
- režim pohybu hmotného majetku,
- režim nakladania s identifikačnými prvkami (kľúče, PIN kódy, identifikačné karty),
- režim obsluhy STO,
- opatrenia a postupy pre mimoriadne situácie. (6)

Pracovníci musia byť preukázateľne oboznámení so stanoveným režimom objektu. (6)

### 1.3.5 Fyzická ochrana

Fyzická ochrana môže byť zabezpečená vlastnými pracovníkmi, alebo zmluvným poskytovateľom bezpečnostných služieb, **lokálne** (na pevných a pohyblivých stanovištiach), **mobilnou hliadkou** (patrolovaním), **diaľkovým bezpečnostným dohľadom,** alebo ich vzájomnou kombináciou. (6)

Ak je fyzická ochrana zabezpečovaná poskytovateľom bezpečnostných služieb, musia byť požiadavky a podmienky výkonu fyzickej ochrany stanovené zmluvným vzťahom, vrátane odbornej spôsobilosti, kvality služieb kontrolných mechanizmov a sankcií. (6)

Doba, rozsah, podmienky výkonu, práva a povinnosti fyzickej ochrany musia byť jednoznačne stanovené, napr. formou smernice pre výkon fyzickej ochrany. (6)

Pri zaistení fyzickej ochrany mimo strážený objekt formou diaľkového bezpečnostného dohľadu prostredníctvom dohľadového centra musí byť prenos poplachového stavu z objektu zabezpečený takým spôsobom, aby nemohlo dôjsť k jeho nekontrolovateľnému prerušeniu (napr. krátky výpadok spojenia s dohľadovým centrom pod.). (6)

Pracovníci fyzickej ochrany:

- kontrolujú vstupy / výstupy osôb,
- kontrolujú vjazdy / výjazdy vozidiel,
- kontrolujú pohyb materiálu do / z objektu (osoby / vozidla),
- zaisťujú správu kľúčov (výdaj / vrátenie a evidenciu),
- zaisťujú informačnú službu,
- vykonávajú kontrolnú obhliadkovú činnosť v stanovených periódach a stanovených trasách,
- identifikujú mimoriadne situácie,
- vykonávajú zákrok v prípade ohrozenia života, zdravia alebo majetku v súlade s postupmi danými bezpečnostnou dokumentáciou,
- vykonávajú ohlasovaciu povinnosť v prípadoch ohrozenia života, zdravia alebo majetku v súlade s postupmi danými bezpečnostnou dokumentáciou,
- prijímajú potrebné opatrenia do času príchodu kvalifikovanej pomoci,
- poskytujú súčinnosť zložkám integrovaného záchranného systému. (6)

## 1.4 Vybrané zákony a európske smernice

Obsahom tejto kapitoly sú vybrané české zákony a nariadenia Európskej únie, ktoré sa vzťahujú k bezpečnosti informácií a zákonu o kybernetickej bezpečnosti č. 181/2014 Sb. (ďalej aj „kybernetický zákon“) a ovplyvňujú systém riadenia bezpečnosti informácií.

### 1.4.1 Národný úrad pre kybernetickú a informačnú bezpečnosť

Kybernetický zákon z časti vychádza z procesných požiadaviek normy ISO / IEC 27000 a zameriava sa na zvýšenie bezpečnosti kritickej infraštruktúry. Dohľad nad kybernetickou bezpečnosťou v Českej republike vykonáva Národný úrad pre kybernetickú a informačnú bezpečnosť (NÚKIB). NÚKIB je ústredným správnym orgánom pre počítačovú bezpečnosť vrátane ochrany utajovaných informácií v oblasti informačných a komunikačných systémov a kryptografické ochrany. Taktiež má na starosti problematiku neverejnej služby v rámci satelitného systému Galileo. Vznikol 1. augusta 2017 na základe zákona č. 205/2017 Sb., ktorým sa zmenil zákon č. 181/2014 Sb. o kybernetickej bezpečnosti a o zmene súvisiacich zákonov. (8)

Hlavné oblasti činnosti NÚKIB:

- prevádzkovať vládny CERT Českej republiky,
- spolupráca s ostatnými národnými CERT tímami a CSIRT tímami,
- spolupráca s medzinárodnými CERT tímami a CSIRT tímami,
- príprava bezpečnostných štandardov pre informačné systémy KII a VIS,
- osveta a podpora vzdelávania v oblasti kybernetickej bezpečnosti,
- výskum a vývoj v oblasti kybernetickej bezpečnosti,
- ochrana utajovaných informácií v oblasti informačných komunikačných systémov,
- kryptografická ochrana,
- národné kontaktné miesto PRS - jedna zo služieb európskeho satelitného systému Galileo (NCPRS). (8)

### 1.4.2 Zákon č.101/2000 Sb.

Všeobecným právnym predpisom ochrany osobných údajov je zákon č. 101/2000 Sb. o ochrane osobných údajov a o zmene niektorých zákonov. Zákon upravuje spracúvanie osobných údajov, ku ktorému môže dochádzať automatizovane alebo inými prostriedkami, štátnymi orgánmi, orgánmi územnej samosprávy, inými orgánmi verejnej moci, ale aj fyzickými a právnickými osobami. Pôsobnosť zákona sa nevzťahuje na náhodné zhromažďovanie osobných údajov, ktoré nie sú ďalej

spracovávané, ani na spracovanie osobných údajov, ktoré vykonáva fyzická osoba výlučne pre osobnú potrebu (14).

Za osobný údaj je podľa zákona považovaná akákoľvek informácia, ak na jej základe možno subjekt údajov priamo alebo nepriamo identifikovať na základe čísla, kódu alebo jedného alebo viacerých prvkov špecifických pre jeho fyzickú, fyziologickú, psychickú, ekonomickú, kultúrnu alebo sociálnu identitu. Zákon rozlišuje osoby, ktoré spracúvajú osobné údaje, na **správcu** a **spracovateľa** osobných údajov. Osoby, ktorých osobné údaje sa spracovávajú, predstavujú podľa zákona dotknuté osoby. Správcom a spracovateľom sú pri ochrane osobných údajov ukladané povinnosti, zatiaľ čo subjektom údajov sú dané práva (14).

### 1.4.3 Všeobecné nariadenie o ochrane osobných údajov

Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27.4.2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov“ tiež známe ako „Všeobecné nariadenie o ochrane osobných údajov“ (General Data Protection Regulation - GDPR) už vstúpila do platnosti a v roku 2018 nastáva transponovanie do českého legislatívneho prostredia. Nariadenie GDPR bude priamo aplikovateľné pre každú organizáciu ponúkajúcu tovary alebo služby v rámci členských štátov Európskej únie a manipulujúci s osobnými údajmi subjektov. Ochrana osobných údajov by mala byť zahrnutá do všetkých firemných procesov a systémov. V rámci novej legislatívy bude celý dodávateľsko-odberateľský reťazec, od výrobcu až po dodávateľov a zákazníkov, zodpovedný za ochranu dát a **nebude možné prevádzať zodpovednosť** za zabezpečenie dát. (11)

Nariadenie prináša subjektom posilnenie existujúcich práv prostredníctvom výrazne väčšej kontroly nad vlastnými osobnými údajmi. Ustanovenie GDPR poskytne fyzickým osobám ľahší prístup k ich dátam, lebo správcovia a spracovatelia dát ich budú musieť dôkladnejšie informovať o spôsobe spracovania informácií, ktorý je dostupný v zrozumiteľnej podobe. Fyzické osoby budú nanovo disponovať právom na **prenosnosť osobných údajov** medzi poskytovateľmi služieb, právom byť **informovaný o zneužití** vlastných dát a právom byť **zabudnutý** pre vymazanie osobných údajov. (11)

Všeobecnou povinnosťou správcu osobných údajov je záväzok zaviesť primerané technické a organizačné opatrenia s cieľom splniť požiadavky nariadenia GDPR pri spracovaní dát a zaručiť ochranu práv dotknutých osôb. Ďalšie povinnosti správcu podľa GDPR zahŕňajú :

- povinnosť vykonať posúdenie vplyvu na ochranu osobných údajov,
- povinnosť viesť záznamy o spracovaniach osobných údajov,
- povinnosť ohlasovať prípady porušenia ochrany osobných údajov,
- povinnosť vymenovať úradníka pre ochranu údajov. (11)

### 1.4.4 Zákon č. 181/2014 Sb.

Dňa 29. augusta 2014 vstúpil do platnosti zákon č. 181/2014 Sb. o kybernetickej bezpečnosti. Zákon nadobudol účinnosť 1. januára 2015. V roku 2017 prebehli dve obsahovo významné novely kybernetického zákona a to prostredníctvom zákona č. 104/2017 Sb. s účinnosťou od 1. júla a zákona č. 205/2017 Sb. s účinnosťou od 1. augusta 2017. Kybernetický zákon upravuje práva a povinnosti osôb, ako aj právomoc a pôsobnosť orgánov verejnej moci v oblasti kybernetickej bezpečnosti. Spracováva príslušné predpisy Európskej únie (jedná sa o transpozícii smernice NIS) a upravuje zaisťovaní bezpečnosti elektronických komunikačných sietí a informačných systémov. (12, 15)

Hlavným cieľom zákona je:

- stanoviť základnú úroveň bezpečnostných opatrení,
- zlepšiť detekciu kybernetických bezpečnostných incidentov,
- zaviesť hlásenia kybernetických bezpečnostných incidentov,
- zaviesť systém opatrení na reakciu na kybernetické bezpečnostné incidenty,
- upraviť činnosť dohľadových pracovísk. (12)

Pôvodné znenie zákona nadobudlo účinnosť 1. januára 2015, aktuálne znenie zákona je účinné od 7. marca 2018. (12)

### 1.4.5 Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148

Dňa 6. júla 2016 bola uverejnená smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 (ďalej len "smernica NIS"). Táto smernica má za cieľ harmonizovať pravidlá členských štátov v oblasti bezpečnosti sietí a informačných systémov a zaviesť jednotný štandard úrovne kybernetickej bezpečnosti s cieľom zlepšiť fungovanie vnútorného trhu. (15)

Niektoré povinnosti, ktoré smernica NIS ukladá, sú v Českej republike už riešené kybernetickým zákonom a jeho vykonávacími predpismi. (15)

Smernica NIS okrem iného rozširuje okruh subjektov, pre ktoré budú stanovené povinnosti v oblasti ochrany a prevencie pred kybernetickými bezpečnostnými incidentmi - jedná sa o tzv. **prevádzkovateľa základnej služby** a **poskytovateľa digitálnych služieb** (internetové vyhľadávače, cloud computing a online trhovisko). Požiadavky smernice NIS zapracováva novela kybernetického zákona cestou zákona č. 205/2017 Sb. s účinnosťou od 1. augusta 2017. Transponujúca lehota na smernicu NIS bola stanovená do 9. mája 2018. (15)

### 1.4.6 Zákon č. 240/2000 Sb.

Zákon č. 240/2000 Sb. o krízovom riadení stanovuje pôsobnosť a právomoc štátnych orgánov a orgánov samosprávy, práva a povinnosti fyzických i právnických osôb pri príprave na kritické situácie, ich riešenie a pri ochrane kritickej infraštruktúry. Vymedzuje povinnosti pre subjekty kritickej infraštruktúry ako správcu kritickej infraštruktúry. Určuje aj zodpovednosť za porušenie týchto povinností. (20)

### 1.4.7 Zákon č. 458/2000 Sb.

Zákon č. 458/2000 Sb. o podmienkach podnikania a o výkone štátnej správy v energetických odvetviach a o zmene niektorých zákonov je základným právnym predpisom, ktorý upravuje energetický sektor v Českej republike. Zákon nadobudol účinnosť 1. januára 2001 a nahradil pôvodný zákon č. 222/1994 Sb. o podmienkach podnikania a o výkone štátnej správy v energetických odvetviach a o Štátnej

energetickej inšpekcii. Do tohto zákona sú implementované jednotlivé právne predpisy Európskej únie, ktoré sa dotýkajú energetických sektorov. (13)

### 1.4.8 Nariadenie vlády č. 432/2010 Sb.

Nariadenie vlády č. 432/2010 Sb. definuje prierezové a odvetvové kritériá na určenie prvku kritickej infraštruktúry. V tejto legislatívnej norme je definovaných 9 odvetví, vrátane jednotlivých sektorových kritérií pre určenie prvku kritickej infraštruktúry. Medzi odvetvia patria:

- Energetika,
- Vodné hospodárstvo,
- Potravinárstvo a poľnohospodárstvo,
- Zdravotníctvo,
- Komunikačné a informačné systémy,
- Finančný trh a mena,
- Núdzové služby,
- Verejná správa. (21)

Toto nariadenie vlády je platné od 30. decembra 2010 a nadobudlo účinnosť 1. januára 2011. V súvislosti so zahrnutím oblasti kybernetickej bezpečnosti do odvetvových kritérií prebehla novela nariadením vlády č. 315/2014 Sb., s účinnosťou od 1. januára 2015. (21)

## 1.5 Analýza a riadenie rizík

Pri zostavovaní vlastnej bezpečnostnej politiky musí byť najprv vykonaná analýza rizík. Musíme teda zistiť, čo a proti čomu (teda aké aktíva proti akým hrozbám) sa chceme chrániť.

Analýza rizík slúži na odhad strát, ktoré môžu vzniknúť pôsobením hrozieb na systém a dáva prehľad o stupni nebezpečnosti jednotlivých hrozieb, o slabých miestach (zraniteľnosti) hodnoteného systému a o rizikách, ktorým je hodnotený systém vystavený. (16)

Riadením rizík sa bližšie zaoberá norma ISO/IEC 27005. Tá proces riadenia rizík definuje nasledovne:

A. stanovenie kontextu,
B. hodnotenie rizík,
   - identifikácia rizík,
   - analýza rizík,
   - vyhodnotenie rizík,
C. ošetrenie rizík,
D. akceptácia rizík. (16)

Proces riadenia rizík informačnej bezpečnosti je nikdy nekončiaci proces a je nutnou súčasťou systému riadenia informačnej bezpečnosti. Pre zabezpečenie tohto procesu sa využíva spomínaný DPCA cyklus. (16)

Hrozby zvyčajne neexistujú izolovane, často ide o kombinácie hrozieb, ktoré predstavujú riziko pre daný subjekt. Pri vykonávaní analýzy rizík je potrebné určiť priority z pohľadu dopadu a pravdepodobnosti ich výskytu a zamerať sa na kľúčové rizikové oblasti. (16)

Norma definuje pravdepodobnosť a mieru rizika nasledovne:

**P - Pravdepodobnosť vzniku a existencie rizika**

1) nepredvídateľná,
2) nepravdepodobná,
3) pravdepodobná,
4) veľmi pravdepodobná,
5) trvalá. (5, 16)

**R - Miera rizika**

1) 0-10: bezvýznamné riziko,
2) 11-20: akceptovateľné riziko,
3) 21-30: mierne riziko,
4) 31-60: nežiaduce riziko,

5) 61-120: neprijateľné riziko. (5, 16)

### 1.5.1 Stanovenie kontextu rizika

Organizácia by mala stanoviť kontext pre riadenie rizík, ktorý definuje rozsah a hranice, zároveň určuje príslušnú organizačnú štruktúru pre riadenie rizík bezpečnosti informácií. Najdôležitejším aspektom je určiť **účel** riadenia rizík bezpečnosti informácií. Medzi účely sa môžu radiť napríklad: právna zhoda a dôkaz povinnej starostlivosti, legislatívna povinnosť, príprava plánu kontinuity činností organizácie, príprava plánu reakcie na incidenty a iné. (16)

### 1.5.2 Hodnotenie rizík

Hodnotenie rizika kvantifikuje alebo kvalitatívne opisuje riziko a umožňuje určiť prioritu rizík podľa ich vnímanej dôležitosti, alebo iných stanovených kritérií. Hodnotenie rizika určuje **hodnotu informačných aktív**, identifikuje možné a existujúce hrozby a zraniteľnosti, určuje existujúce opatrenia a ich účinok na riziko, determinuje potencionálne dopady a ustanovuje prioritu určených rizík. (16)

#### a) Identifikácia rizík

Účelom identifikácie rizík je určiť príčiny vzniku potencionálnej straty a porozumieť všetkým okolnostiam, pri ktorých môže dôjsť k strate. V nasledujúcich odsekoch sú opísané kroky na zhromaždenie vstupných dát pre činnosť posúdenia rizika. (16)

#### Identifikácia a hodnotenie aktív

Pod aktívom si možno predstaviť všetok hmotný a nehmotný majetok, ktorý má pre organizáciu hodnotu a vyžaduje ochranu. Pre ohodnotenie aktív je nevyhnutné najprv identifikovať aktíva. Identifikácia aktív sa vykonáva na vhodnom stupni podrobnosti, ktorý poskytuje pre hodnotenie rizika dostatok informácií. Stupeň podrobnosti možno spresniť v ďalšom opakovaní hodnotenia rizík. V tejto etape sa odporúča zoskupiť všetky aktíva, ktoré k sebe logicky patria. Zoznam identifikovaných aktív musí obsahovať vlastníka aktíva, ktorým sa rozumie poverená osoba, zodpovedná za jeho

produkciu, vývoj, údržbu, používanie a bezpečnosť. Vlastník aktíva je najvhodnejšou osobou, ktorá dokáže určiť hodnotu aktíva pre organizáciu. (16)

Po vytvorení zoznamu aktív je potrebné k ohodnoteniu aktív stanoviť stupnicu, na základe ktorej budú dané riziká hodnotené a hodnotiace kritériá pre každý stupeň. Stupnica môže byť vyjadrená finančnými čiastkami, či kvalitatívnymi hodnotami a obe varianty možno kombinovať. **Peňažná stupnica** vyjadruje hodnotu určitého aktíva, zatiaľ čo **kvalitatívna stupnica** reprezentuje hodnotu pomocou termínov, napríklad od veľmi nízkej až po kritickú. Dôležité je vhodné farebné odlíšenie pre lepšiu orientáciu v rozsiahlych tabuľkách s hodnotením aktív. Rozsah a výber termínov si môže organizácia zvoliť v závislosti na bezpečnostných potrebách alebo svojej veľkosti. (16)

Tabuľka 4: Číselné a slovné vyjadrenie hodnoty rizík (vlastné spracovanie)

| HODNOTA | ČÍSELNÉ VYJADRENIE | SLOVNÉ VYJADRENIE |
|---|---|---|
| 1 | 0 % - 30 % | Nízka pravdepodobnosť |
| 2 | 30 % - 65 % | Stredná pravdepodobnosť |
| 3 | 65 % - 100 % | Vysoká pravdepodobnosť |

**Identifikácia a posúdenie hrozieb**

Hrozba má potencionálnu schopnosť poškodiť aktíva, ako sú informácie, procesy a systémy, tým aj samotnú organizáciu. Podľa pôvodu možno hrozby rozdeliť na prírodné alebo spôsobené ľudským faktorom. Podľa úmyslu sa hrozby rozlišujú na **náhodné** a **úmyselné**. Z hľadiska bezpečnosti je žiadúce, aby náhodné a úmyselné hrozby boli identifikované spoločne s odhadom ich úrovne a pravdepodobnosti. Hrozby by sa mali identifikovať podľa typu, či v prípade potreby určiť jednotlivé hrozby v rámci všeobecnej triedy. V praxi je odporúčané zoskupenie hrozieb podľa aktív, na ktoré hrozba pôsobí. (16)

Hodnotenie hrozieb sa vykonáva z pohľadu možného narušenia **dostupnosti, dôvernosti, integrity** aktív. Pri posudzovaní sa nesmie zabudnúť na tzv. následné efekty hrozby a vždy je potreba premyslieť možné vplyvy hrozieb do najmenších podrobností. Napríklad výpadok elektrickej energie neznamená len nedostupnosť dát,

ale môže viesť pri dlhodobom výpadku k ohrozeniu činnosti organizácie, prípadne aj ohrozenie fyzickej integrity človeka. (16)

**b) Analýza rizík**

Analýza rizík sa vykonáva v rôznych stupňoch podrobnosti v závislosti na kritickosti aktív, rozsahu zrejmej zraniteľnosti a predchádzajúcich incidentoch zasahujúcich organizáciu, či skupinu organizácií, za účelom identifikácie zraniteľných miest a pôsobiacich hrozieb. **Cieľom analýzy** rizík je **zníženie veľkosti rizika na prijateľnú úroveň**, respektíve prijatie zvyškových rizík, pri ktorých je eliminácia rizika neefektívna. Forma analýzy rizík by mala byť súčasťou pri stanovení kontextu. (16)

Metodiky analýzy rizík môžu byť **kvalitatívne** alebo **kvantitatívne**, ale v závislosti od okolností je možné použiť kombináciu oboch metodík. Kvalitatívna analýza je zvyčajne menej zložitá a nákladná ako kvantitatívna analýza. V praxi sa často používa najprv kvalitatívna analýza k získaniu všeobecnej indikácie úrovne rizika a k odhaleniu väčších rizík, pričom neskôr môže byť potrebné vykonať viac konkrétnu, alebo kvantitatívnu analýzu k upresneniu rizík. (16)

**Kvalitatívna analýza** rizík používa na opis veľkosti následkov a pravdepodobnosti stupnicu alebo škálu, ktorú je možné prispôsobiť podľa okolností a pre rôzne riziká možno použiť rôzne popisy. Výhodou kvalitatívnej metódy je jednoduché použitie a jej nevýhodou je závislosť na subjektívnom výbere hodnotiacej škály. Kvalitatívna analýza rizík môže byť použitá v prípade, keď sú zdroje číselných údajov nevhodné, alebo pri počiatočnom určení rizík, ktoré vyžadujú podrobnejšiu analýzu . (5, 16)

**Kvantitatívna analýza** rizík používa pre veľkosť následkov a pravdepodobnosti stupnicu s číselnými hodnotami. Kvalita analýzy závisí od presnosti a úplnosti číselných hodnôt a platnosti použitých modelov. Pri kvantitatívnej analýze rizík možno vychádzať z historických dát incidentov a medzi jej výhody sa radí presné vyčíslenie škôd spôsobených naplnením rizika. Nevýhodou kvantitatívneho prístupu je nedostatok dát pri nových rizikách a o slabých miestach v bezpečnosti, alebo nedostupnosť konkrétnych a kontrolovaných dát, čo vytvára mylný dojem o význame a presnosti hodnotenia rizík. (5, 16)

### c) Hodnotenie rizík

Výstupom analýzy rizík je zoznam rizík s pridelenou prioritou podľa kritérií hodnotenia rizík v súvislosti so scenármi incidentov, ktoré k týmto rizikám vedú. O hodnotení rizík by organizácia mala porovnať odhadnuté riziká s kritériami hodnotenia rizík definovaných počas stanovenia kontextu. (16)

Jedným z možných prístupov k hodnoteniu rizík je **metóda vyhodnocujúca pravdepodobnosť incidentu a jeho vplyv**. Táto metóda využíva dva parametre, ktorými sú pravdepodobnosť a dopad incidentu a skladá sa zo štyroch etáp. Prvým krokom je doplnenie existujúcich opatrení do tabuľky hrozieb a zraniteľností. Následne je vykonaný odhad pravdepodobnosti incidentu. Na záver je vypočítaná miera rizika pomocou vzťahu $\boldsymbol{R = PI \cdot D}$, pričom $R$ predstavuje miera rizika, $PI$ pravdepodobnosť incidentu a $D$ dopad. (16)

## 1.5.3 Ošetrenie rizík

Pre proces ošetrenia rizík je nutný zoznam jednotlivých rizík, ktorým bola udelená priorita podľa kritérií hodnotenia rizík v súvislosti so scenármi incidentov. K dispozícii sú 4 voľby ošetrenia rizík: modifikácia rizika, podstúpenie rizika, vyhnutie sa riziku a zdieľanie rizika. Spôsob ošetrenia jednotlivých rizík by sa mal vyberať na základe výsledkov z hodnotenia rizík, očakávaných nákladov na implementáciu a očakávaných prínosov, plynúcich z týchto spôsobov. (16)

**Modifikácia rizika** - úroveň rizika by mala byť riadená zavedením, odstránením, alebo zmenou opatrenia, aby bolo zvyškové riziko prehodnotené na prijateľné. (16)

**Podstúpenie rizika** - keď úroveň rizík spĺňa kritériá akceptácie rizika, nie je potrebné prijímať ďalšie opatrenia a riziko možno podstúpiť. (16)

**Vyhnutie sa riziku** - organizácia môže prijať rozhodnutie o celkovom vyhnutí sa riziku zmenou podmienok plánovanej alebo existujúcej činnosti, ak sú identifikované riziká považované za príliš vysoké, alebo náklady na ošetrenie rizík prevyšujú prínosy. (16)

**Zdieľanie rizika** - zahŕňa rozhodnutie zdieľať určité riziká s externými stranami, pričom môžu vznikať nové riziká, alebo sa môžu meniť existujúce. Preto môže byť potrebné ďalšie ošetrenie rizík. Zodpovednosť za zvládnutie rizika je možné zdieľať, ale zodpovednosť za dopad zvyčajne zdieľať nemožno. (16)

### 1.5.4 Akceptácia rizík

Plány ošetrenia rizík opisujú spôsob ošetrenia hodnotených rizík, aby spĺňali kritériá pre akceptáciu rizika. Oprávnené osoby, zvyčajne vedúci pracovníci, prehodnocujú a schvaľujú plány ošetrenia rizík a výsledné zvyškové riziká. Zoznam akceptovaných rizík a zodpovednosti za tieto rozhodnutia musia byť oficiálne formálne zaznamenané. V niektorých prípadoch nemusí úroveň zvyškového rizika spĺňať kritériá akceptácie rizika, pretože uplatňované kritériá nezohľadňujú prevažujúce okolnosti, naznačujúce neprimeranosť kritérií akceptácie rizík. (5, 16)

Výstupom je zoznam akceptovaných rizík s odôvodnením pre tie, ktoré nespĺňajú bežné kritériá akceptácie rizík organizácie. (16)

# 2 ANALÝZA SÚČASNÉHO STAVU

Nakoľko táto práca sa týka elektronických zabezpečovacích systémov pre objekty kritickej infraštruktúry, tak aj táto analýza bude zameraná výhradne na prvky KI. V tejto časti bude popísaná realizovaná analýza odvetvia, legislatívy, súčasného stavu a ochrany prvkov kritickej infraštruktúry. Problematiku fyzickej bezpečnosti, ako súčasť kybernetickej bezpečnosti, riešia všetky prenosové a distribučné spoločnosti energií naprieč celou Českou republikou.

Je nutné poznamenať, že nižšie uvedené informácie, skutočnosti pochádzajú z konkrétnej spoločnosti, ktorú nie je možné z titulu zásad ochrany utajovaných údajov konkretizovať.

## 2.1 Analýza odvetvia z pohľadu energetiky

Nasledujúce podkapitoly sa zaoberajú analýzou odvetvia energetiky v Českej republike so zameraním na elektroenergetiku, subjekty vystupujúce na trhu, významné zákony a regulácie subjektov na trhu. Uvedené poznatky vychádzajú zo zákona č. 458/2000 Sb. o podmienkach podnikania a o výkone štátnej správy v energetických odvetviach (ďalej len „energetický zákon“).

### 2.1.1 Subjekty v odvetví elektroenergetiky

Základné členenie subjektov vystupujúcich na trhu rozdeľujeme do skupín:

- výrobcovia elektriny,
- prevádzkovateľ prenosovej sústavy,
- prevádzkovatelia distribučných sústav,
- operátor trhu,
- obchodníci s elektrinou,
- zákazníci. (13)

Podnikať v odvetví energetiky na území Českej republiky môžu fyzické alebo právnické osoby na základe licencie udelenej Energetickým regulačným úradom. Predmetom podnikania v energetických odvetviach je: výroba elektriny, prenos elektriny, distribúcia elektriny, činnosti operátora trhu, výroba plynu, preprava plynu, distribúcia plynu, uskladňovanie plynu a obchod s plynom a výroba tepelnej energie a rozvod tepelnej energie. (13)

Medzi podmienky pre udelenie licencie fyzickej osobe patrí: dosiahnutie plnoletosti, právna spôsobilosť, trestná bezúhonnosť a odborná spôsobilosť. Právnické osoby sú povinné ustanoviť zodpovedného zástupcu a uvedené požiadavky na fyzickú osobu musia spĺňať členovia štatutárneho orgánu. Licencia sa udeľuje na základe písomnej žiadosti. (13)

### 2.1.2 Výrobca elektriny

Výrobca elektrickej energie musí na pripojenie k elektrizačnej sústave spĺňať technické požiadavky na prevádzkovanie prenosovej alebo distribučnej sústavy. Podmienkou pre výrobcov elektriny je **získanie licencie** a **registrácia u operátora trhu.** Výrobca elektriny sa musí riadiť pokynmi technického dispečingu prevádzkovateľa prenosovej alebo distribučnej sústavy, ku ktorej je výrobňa elektriny pripojená, ďalej poskytovať potrebné informácie pre prevádzku, dispečerské riadenie a rozvoj prenosovej sústavy alebo distribučnej sústavy, tiež i operátorovi trhu údaje potrebné pre plnenie ich povinností. (13)

### 2.1.3 Prevádzkovateľ prenosovej sústavy

Prenosová sústava je prepojená medzi európskymi elektrizačnými sústavami a slúžia pre zaistenie prenosu elektriny od výrobcu k distribútorovi na celom území Českej republiky, kde prevádzkovateľom prenosovej sústavy je jedna spoločnosť s jediným akcionárom, ktorým je štát Českej republiky. Prevádzkovateľ prenosovej sústavy riadi toky elektriny v prenosovej sústave a musí pritom rešpektovať prenosy elektriny medzi prepojenými sústavami ostatných štátov v spolupráci s prevádzkovateľmi distribučných sústav v elektrizačnej sústave v rámci Českej republiky. (13)

Plnenie, dozor a celkovú činnosť v spoločnosti vykonáva Ministerstvo priemyslu a obchodu. Prevádzkovateľ prenosovej sústavy podľa energetického zákona musí byť z hľadiska svojej spoločenskej štruktúry nezávislý na výrobe a obchode s elektrinou a plynom a mať pridelený certifikát nezávislosti. (13)

### 2.1.4 Prevádzkovateľ distribučnej sústavy

Distribučnú sústavu tvoria spoločnosti, čo zabezpečujú prenos z prenosovej sústavy, alebo zo zdrojov, do nich zapojených (elektrárne) ku koncovým užívateľom. Súčasťou distribučnej sústavy sú aj jej riadiace, ochranné, zabezpečovacie a informačné systémy. Prevádzkovateľ distribučnej sústavy zaisťuje spoľahlivé prevádzkovanie, obnovu a rozvoj distribučnej sústavy na území vymedzenom licenciou. Prevádzkovateľ distribučnej sústavy, ktorý má viac ako 90 000 odberných miest, nesmie byť súčasne držiteľom licencie na výrobu elektriny, prenos elektriny, obchod s elektrinou či s plynom. Medzi výhody distribútora podľa zákona patrí možnosť nakupovať s najnižšími nákladmi podporné služby a elektrinu pre krytie strát elektriny v distribučnej sústave. (13)

### 2.1.5 Operátor trhu

Operátorom trhu je akciová spoločnosť, ktorej zakladateľom je štát Česká republika. Štát vlastní akcie operátora trhu, ktorých celková menovitá hodnota predstavuje najmenej 67% základného imania operátora trhu. Podobne, ako pri spoločnosti zabezpečujúcej prenosovú sústavu v ČR, tak aj tu plnenie, dozor a celkovú činnosť v spoločnosti vykonáva Ministerstvo priemyslu a obchodu. (13)

**Predmet činnosti** operátora trhu vychádza z energetického zákona, pričom medzi jeho hlavné funkcie patria: organizovanie krátkodobého trhu s elektrickou energiou a plynom, sprostredkovanie obchodu s elektrickou energiou, poskytovanie záruky na pôvod elektriny z obnoviteľných zdrojov, evidencia výrobnej elektriny, spracovanie obchodných podmienok operátora trhu pre elektrickú energiu a pre plynárenstvo, či tvorba správ o trhu s elektrickou energiou a plynom. (13)

K ďalším činnostiam patrí: informovať prevádzkovateľa prenosovej sústavy, prevádzkovateľa prepravnej siete a prevádzkovateľa zásobníkov plynu alebo prevádzkovateľa distribučnej sústavy o neplnení platobných povinností účastníkov trhu a subjektov zúčtovania voči operátorovi trhu. To spracovávať a odovzdávať ministerstvu, Energetickému regulačnému úradu, prevádzkovateľmi prenosovej sústavy a prevádzkovateľovi prepravnej sústavy aspoň raz ročne správu o budúcej očakávanej spotrebe elektriny a plynu a o spôsobe zabezpečenia rovnováhy medzi ponukou a dopytom elektriny a plynu. (13)

### 2.1.6 Obchodník s elektrinou

Obchodník predstavuje fyzickú alebo právnickú osobu, ktorá nakupuje elektrinu za účelom jej predaja. Energie sa predávajú ako komodity. Medzi práva obchodníka s elektrinou patrí umožnenie prenosu alebo distribúcie elektriny spoločnosťami, nakupovať elektrinu od držiteľov licencie na výrobu či obchod elektrickej energie, alebo z iných štátov, predávať ju ostatným účastníkom trhu. Obchodník s elektrinou musí od energetického regulačného úradu získať licenciu, ktorá má obmedzenú platnosť a to päť rokov. Po vypršaní licencie musí subjekt písomne zažiadať o obnovenie. (13)

### 2.1.7 Zákazníci

Zákazník je osoba, ktorá nakupuje elektrinu pre svoje vlastné konečné použitie v odbernom mieste. Všetci zákazníci pritom majú na energetickom trhu rovnaké práva a povinnosti, ktorých garantom je Energetický regulačný úrad. (13)

## 2.2 Legislatíva a regulácia ovplyvňujúca energetiku

Alfou a omegou pre energetický trh je energetický zákon 458/2000 Sb., Zákon o podmienkach podnikania a o výkone štátnej správy v energetických odvetviach a o zmene niektorých zákonov, ktorý doplňujú vyhlášky. Je potrebné sledovať meniacu sa legislatívu v odvetví a to napríklad: cenové rozhodnutie Energetického regulačného úradu, nové nariadenia vlády, zákon o hospodárení energií, vyhlášky k energetickému zákonu, či vyhlášky Ministerstva priemyslu a obchodu.

Okrem legislatívne stanovených práv a povinností ako je: ochrana spotrebiteľa, daňová legislatíva a pod., energetické odvetvie je ovplyvňované cenovou reguláciou a kontrolami vstupu do odvetvia prostredníctvom udeľovania licencií na výkon činnosti na základe štátneho súhlasu. Podstatná je aj väzba na ochranu životného prostredia, ktorej súčasťou sú nariadenia na zníženie emisií skleníkových plynov, zvýšenie energetickej účinnosti a zvýšenie podielu obnoviteľných zdrojov energie na celkovej spotrebe. Hlavnými orgánmi štátnej správy pre oblasť regulácie sú **Energetický regulačný úrad** a **Ministerstvo priemyslu a obchodu.**

### 2.2.1 Energetický regulačný úrad

Energetický regulačný úrad pôsobí ako správny úrad pre výkon regulácie v energetike. Medzi hlavné oblasti pôsobnosti patrí: regulácia cien, monitorovanie a vyhodnocovanie dodržiavania kvality dodávok a služieb v elektroenergetike a plynárenstve, rozhodovanie o potrebných licenciách a certifikátoch nezávislosti, podpora hospodárskej súťaže v energetických odvetviach, v neposlednom rade i **výkon dohľadu nad trhmi v energetických odvetviach.** (13)

### 2.2.2 Ministerstvo priemyslu a obchodu

Ministerstvo priemyslu a obchodu v odvetví poskytuje štátnu autorizáciu na výstavbu výrobnej elektriny a plynových zariadení, vypracúva štátnu energetickú koncepciu a národný akčný plán pre energiu z obnoviteľných zdrojov, spracováva analýzy zavedenia inteligentných meracích systémov v oblasti elektroenergetiky a plynárenstva, zabezpečuje plnenie záväzkov vyplývajúcich z medzinárodných zmlúv, alebo z členstva v medzinárodných organizáciách a predovšetkým vydáva vyhlášky. (13)

## 2.3 Základný popis spoločnosti

Energetická spoločnosť, pre ktorú je táto práca spracovaná, je súčasťou medzinárodného energetického koncernu pôsobiaceho v mnohých krajinách Európy, z časti v Rusku a Severnej Amerike. Aktivity spoločnosti sú na území Českej republiky usmerňované matkinou holdingovou spoločnosťou, sídliacou mimo ČR. Organizačné

usporiadanie je zostavené tak, aby jasne vymedzovalo úlohy a zodpovednosti individuálnych spoločností v rámci holdingu, ktorých spolupráca je založená na základe uzatvorených zmlúv o poskytovaní služieb.

Medzi hlavné činnosti jednotlivých spoločností sa radia: realizácia strategických rozhodnutí a podpora operačných činností obchodovania a distribučné spoločnosti, obchodovanie s elektrickou energiou a plynom, výroba elektrickej a tepelnej energie, prevádzka, rozvoj a údržba elektrickej a plynovej distribučnej sústavy, servisné služby a opravy v oblasti distribúcie elektriny a plynu, alebo poskytovanie IT a telekomunikačných služieb v skupine.

## 2.4 Popis objektov kritickej infraštruktúry

Je dôležité uviesť, že spoločnosť je vlastníkom objektov KI , preto úplne zodpovedá za ich správu a prevádzku, a teda patria podľa Nariadenia vlády č. 315/2014 Sb. medzi prvky Kritickej infraštruktúry Českej republiky.

Ide o objekty, ako sú: rozvodne elektrickej energie (rozvodné stanice), prepínacie stanice, trafostanice, vonkajšie káblové vedenie, elektrárne apod. (19)

### 2.4.1 Rozvodne elektrickej energie

Z historického a časového hľadiska sú objekty rôznorodé, či už rozlohou, architektonickým návrhom, alebo použitými technológiami. Preto táto analýza súčasného stavu popisuje priemerný stav rozvodní, ich režim fungovania a technický stav.

Tieto rozvodné stanice (RS) sa spravidla nachádzajú na okrajoch väčších miest, či v blízkosti veľkoodberateľov, ale i v tesnej blízkosti elektrární alebo rozvodní prenosovej sústavy.

**Delenie rozvodných staníc**

Z pohľadu časti technológií VVN a VN sa RS delia základné typy a tými sú vonkajšie a zapuzdrené. **Vonkajšie** sú umiestnené na odľahlých miestach, alebo okrajových

častiach mesta. Vedenie elektrickej energie je buď **káblové** (uložené v zemi), alebo **vonkajšie** (holé vodiče na podperných stĺpoch). Spravidla k nim vedie vonkajšie káblové vedenie vedené na podperných stĺpoch. Naopak **zapuzdrené** stanice sa nachádzajú v priestoroch väčších miest, kde nie je dostatočný vhodný priestor pre vybudovanie vonkajších RS. Princíp vedenia energie je taký, že do stanice vedú silové káble, uložené v zemi. Často krát sa tieto RS nachádzajú v blízkosti biznis centier, alebo vo veľkých administratívnych a výrobných oblastiach. Perimeter vonkajších staníc chráni plot s ostnatým drôtom a samotnú technológiu (umiestenú vo vonkajších priestoroch objektu) a chráni ešte vnútorné oplotenie, ktoré skôr nadobúda varovný charakter „zákaz vstupu“ z pohľadu BOZP. Zapuzdrené rozvodne sú zvyčajne umiestené v priestoroch budov, kde je vyhradený jeden hlavný vstup a únikové východy. Perimeter chránia steny budovy a oceľové vstupné dvere. V niektorých prípadoch sú tiež inštalované okná, ktoré sú zväčša umiestnené v bezpečnostnej výške nad 3 metre.

**Vstupy do objektu**

Do objektov rozvodní majú prístup výhradne len poverené a oprávnené osoby. V prípade potreby asistencie tretích strán, pri oprave a rekonštrukcii priestorov, alebo návšteve, je spísaný zoznam osôb, ktorý je predložený miestnemu správcovi rozvodne. Pre vstup do rozvodne je potrebné splňovať § 4, vyhlášky č. 50/1978 Sb. Českého úradu bezpečnosti práce a Českého banského úradu o odbornej spôsobilosti v elektrotechnike, ale len za sprievodu osoby s § 6 tej istej vyhlášky a vyšším. V opačnom prípade musí poverený pracovník spoločnosti dozerať na práce vykonané tretími stranami a sprevádzať osoby, ktoré sú na návšteve.

Samotný prístup do vybraných objektov je riešený pomocou čipovej karty napojenej na PZTS, alebo bezpečnostných zámkov a kľúčov a PIN. Čipové karty slúžia na identifikáciu oprávneného vstupu pracovníka do objektu, taktiež pre aktiváciu a deaktiváciu prvkov PZTS. Do priestoru rozvodne sa spravidla vstupuje príjazdovou komunikáciou, kde je pojazdná brána s čítačkou kariet. Hlavný vstup do budovy sa odomyká a zamyká automaticky po priložení čipovej karty s oprávnením vstupu. Ten istý princíp sa využíva aj pri odchode z rozvodne. Pri výjazde z areálu pracovník počká a skontroluje, či sa pojazdná brána dokonale zavrela. Druhý spomínaný prístup sa

využíva len v nevyhnutných a naliehavých prípadoch. Spôsob vynecháva použitie čipovej karty, ale prebieha klasickým otvorením brány a vstupných dverí mechanickým kľúčom. Pri tomto spôsobe je nutné deaktivovať zabezpečenie ručne, a to zadaním PIN na klávesnici, ktorá riadi ústredňu PZTS. Pri odchode z miesta je taktiež nutné objektu aktivovať zabezpečenie, a to rovnakým spôsobom. Následne plynie časový úsek, kedy osoba musí opustiť priestory budovy. V opačnom prípade sa spustí poplach.

**Režim obsluhy**

Režim obsluhy popisuje intenzitu potreby pracovníkov na mieste RS. V spoločnosti je snaha inovovať a prevádzkovať tzv. bezobslužné rozvodne. Je nutné dodať, že prevažná väčšina staníc je vonkajšieho typu, preto tam rastie tráva, ktorú treba kosiť. Táto činnosť si vyžaduje prístup personálu do areálu.

Nasledovný zoznam popisuje kategórie režimu obsluhy:

1) bez stálej obsluhy - manipulácia podľa požiadavky dispečera, diaľkové ovládanie,
2) kontrola 1 x za týždeň, manipulácia podľa požiadavky dispečera, diaľkové ovládanie,
3) obsluha prítomná denne v čase od 6.00 do 14.00 hod., mimo túto dobu bez, manipulácia na požiadavku dispečera, diaľkové ovládanie,
4) trvalá obsluha 24 hodín denne, neustály dohľad nad RS v danej oblasti, pohotovostný dispečing.

### 2.4.2 Transformačné stanice

Transformačná stanica, známa tiež ako trafostanica, je zariadenie, ktoré za pomoci transformátora mení vysoké napätie (22 kV) na nízke napätie (400 V, 230 V). Každá trafostanica je na jednej strane spojená s rozvodňou pomocou VN vedenia, následne nastáva transformácia napätia a z nej potom vedie NN ku koncovým zákazníkom (prevažne domácnostiam). Veľkí a významní odberatelia môžu disponovať vlastnými trafostanicami.

Trafostanice majú formu samostatného uzavretého objektu, môžu byť integrovanou súčasťou iného (aj cudzieho) objektu, alebo sú umiestnené vonku na podporných

stĺpoch vedenia VN. Do uzavretej trafostanice má prístup len technik (pomocou špeciálneho kľúča), ktorý do nej vstupuje len za účelom revízie, údržby alebo opravy. Vonkajšie trafostanice sú umiestnené na stĺpoch v tzv. bezpečnostnej výške, aby boli bez ďalšieho vybavenia pre človeka ťažko dosiahnuteľné, v tom prípade hovoríme o ochrane polohou.

### 2.4.3 Vonkajšie a káblové vedenie

Vonkajšie a káblové vedenie slúži na spájanie výrobcu elektrickej energie, prenosovej sústavy, distribučnej sústavy až ku konečnému zákazníkovi. Vedenie sa rozdeľuje do kategórií:

- vedenie UNV (ultra-vysoké napätie) - napätie medzi vodičmi nad 800 kV,
- vedenie ZVN (zvlášť vysoké napätie) - 300 až 800 kV,
- vedenie VVN (veľmi vysoké napätie) - 52 až 300 kV,
- vedenie VN (vysoké napätie) - 1 000 V až 52 kV,
- vedenie NN (nízke napätie) - 50 až 1 000 V,
- vedenie MN (malé napätie) do 50 V.

Z hľadiska rozmiestnenia všetky viditeľné trasy elektrického vedenia vo voľnej krajine patria distribučnej spoločnosti pre danú oblasť. V mestách a obývaných oblastiach, kde je hustá výstavba, sa trasy vedú v podzemných káblových kanáloch.

Vonkajšie i káblové vedenie je navrhnuté tak, aby človeku pri bežnom správaní nehrozil úraz elektrickým prúdom a ani ho nemohol nijako poškodiť, taktiež ide o ochranu polohou. Technici musia pri údržbe a opravách elektrického vedenia používať špeciálne prostriedky na to určené.

## 2.5 7S analýza spoločnosti

Analýza interných faktorov – model McKinsey 7S hodnotí spoločnosť z pohľadu siedmich nižšie uvedených faktorov.

### 2.5.1 Stratégia

Stratégiou spoločnosti je dlhodobo udržiavať a rozvíjať distribučnú sústavu na spravovanom území a byť minimálne v týchto regiónoch jednotkou na trhu dodávateľov energií.

**Poslaním** firmy v Českej republike je zaistiť spoľahlivú prevádzku, optimalizáciu procesov a modernizáciu infraštruktúry. Aktivity ES sú na českom trhu smerované k dosiahnutiu vedúceho postavenia v oblastiach zákazníckej orientácie a energeticky efektívnych riešení.

**Vízia** firmy je vytvoriť natrvalo udržateľné riešenia, obnoviteľné a decentralizované zdroje, energetickú efektivitu a lokálne energetické systémy. Taktiež víziou je zažívať dynamickejší rast a hrať čoraz dôležitejšiu úlohu v mnohých krajinách.

### 2.5.2 Štruktúra

Právna forma, štruktúra, je akciová spoločnosť a patrí do skupiny spoločností, ktoré tvoria holding. Vedenie spoločnosti tvorí predstavenstvo, ktoré je tvorené z troch pozícií: predseda, podpredseda a členovia predstavenstva. Jednotlivé činnosti spoločnosti sa rozdeľujú do samostatných oblastí, ktoré spracúvajú do rozličných útvarov so vzájomnou kooperáciou.

### 2.5.3 Systémy

V spoločnosti už sú zavedené určité EZS a systémy kontroly vstupu (ďalej len SKV), avšak sú zavedené sporadicky, nesystematicky, ktoré boli nasadené v priebehu času bez inovácie, takže sú zastarané. SKV je zavedený v administratívnych centrách a na vybraných objektoch KI. Každý objekt obsahujúci EZS je vybavený ústredňou poplašných zabezpečovacích a tiesňových systémov (ďalej len PZTS) a tá spracúva signály ako z EZS, tak aj z SKV. Pre vstup do objektov KI je nutná čipová karta s oprávneným vstupom.

### 2.5.4 Štýl riadenia

Jednotlivé útvary riadia vedúci daných útvarov. Konečné návrhy a rozhodnutia schvaľuje predstavenstvo firmy. Dohľad nad činnosťou spoločnosti zabezpečuje dozorná rada tvorená členmi nadradených spoločností koncernu a členmi príbuzných spoločností v rámci holdingu. V najvyšších sférach manažmentu sa uplatňuje autokratický štýl riadenia, v strednom manažmente prevažuje demokratický štýl, avšak nie je to pravidlo.

### 2.5.5 Spolupracovníci

V spoločnosti pracuje približne 400 zamestnancov rôznorodého zamerania v energetickom prostredí, ktorí sa rozdeľujú na kmeňových a agentúrnych zamestnancov. Spoločnosť ďalej poskytuje študentom možnosti štipendií, pracovné stáže a tzv. trainee programy. Spôsob výberu zamestnancov je individuálny na základe požadovanej pracovnej pozície, avšak všeobecne prebieha ústnym pohovorom s vedúcim teamu, ktorý prakticky preverí potrebné skúsenosti uchádzača na danú pozíciu. V spoločnosti vysoko dbajú na osobný rozvoj zamestnancov, z toho dôvodu sa pravidelne konajú rôzne školenia, či už odborného zamerania, alebo školenia pre osobný rozvoj.

### 2.5.6 Schopnosti

Je nutné podotknúť, že spoločnosť patrí do holdingu a na trhu pôsobia ako celok. Celý kolektív spoločnosti je na vysokej profesionálnej úrovni, o ktorej svedčia referencie spokojných zákazníkov. Pre zlepšenie zručností sa pracovníci zúčastňujú výstav, veľtrhov a školení na nové technológie. Z pohľadu informačných technológií ide o pokročilých používateľov. Niektorí už majú skúsenosti s EZS, preto by nemal byť problém so zavedením a prevádzkou nových systémov.

### 2.5.7 Zdieľané hodnoty

Veľká väčšina zamestnancov zdieľa hodnoty definované v poslaní, vízii a strategických cieľoch spoločnosti odvedením kvalitnej práce s vysokou pridanou hodnotou pre zákazníka a šíria tak dobré meno spoločnosti, čo svedčí o ich vysokej lojalite.

## 2.6 Analýza IS/IT spoločnosti

Kapitola sa zaoberá analýzou IS / IT spoločnosti pomocou identifikácie súčasného stavu.

### 2.6.1 Analýza prvkov EKV

Systém kontroly vstupu je implementovaný v niektorých objektoch KI a veľkých administratívnych strediskách, kde sa používajú zamestnanecké karty na vstup do vybraných častí týchto objektov. Bohužiaľ, momentálny stav je taký, že v dôsledku občasného premiestňovania niektorých oddelení v rámci budov a fluktuácií zamestnancov sa prideľujú oprávnenia podľa potreby. Aktuálne nie je spracovaný hierarchický zoznam užívateľov a ich právomocí na vstup do vybraných zón objektu. Je teda veľmi pravdepodobné, že niektorí zamestnanci majú prístup tam, kde už pracovne nepôsobia (v rámci objektu alebo niekoľkých objektov) a to z dôvodu, že tieto objekty alebo zóny niekedy v minulosti využívali. Po správnosti by tieto prístupy mali byť časovo ohraničené, alebo ručne odstránené po zániku vzťahu zamestnanca k týmto priestorom, avšak to sa momentálne nedeje.

Ďalej je systém kontroly vstupu implementovaný ako súčasť PZTS v budovách KI. Taktiež sa tu využívajú zamestnanecké karty. Pokus o neoprávnený prístup je detekovaný, zaznamenaný a prenesený do systému ABI. Do objektov KI je možné vstúpiť taktiež pomocou fyzického kľúča a deaktivovať zabezpečenie PZTS pomocou PIN kódu a klávesnice. Vjazdy a výjazdy do priestorov KI tú taktiež vybavené čítačkami kariet s napojením na PZTS a automatizovanými pojazdnými bránami.

### 2.6.2 Analýza prvkov PZTS

Z historického hľadiska boli zabezpečovacie systémy realizované v rôznych objektoch oblastných rozvodní rôznymi dodávateľmi, hlavne z dôvodu ochrany majetku a osôb pred zlodejmi a záškodníkmi. Použité prvky v PZTS sú generačne rozdielne, ich funkcionalita, technické parametre, výkon sú tiež v priebehu času rozdielne. Služby ohľadom správy a projekcie systémov PZTS sú „outsoucované“ jednej konkrétnej

dodávateľskej spoločnosti. Na pulty centrálnej ochrany, umiestnené v priestoroch oblastných rozvodní, sú napojené všetky PZTS z jednotlivých objektov.

Hlášky a signály o narušení z ústrední PZTS v rozvodni putujú k pracovníkom **tromi** spôsobmi**. Prvý prípad** je priamo na dispečing v danej oblasti oblastných rozvodní. Toto hlásenie sa zobrazuje priamo na pulte centrálnej ochrany 24 hodinovej pohotovosti. **Druhý spôsob** je cez siete GSM a hlásenia chodia zamestnancom, ktorí majú pohotovosť, priamo na mobil prostredníctvom SMS s obsahujúcou správou „narušenie objektu – rozvodňa (názov)“. **Tretí** smer hlásení sa zbieha, zaznamenáva a uchováva v systéme pre správu PZTS a EKV – Advanced building intelligence (ABI).

### 2.6.3 Analýza prvkov CCTV

Technológie pre kamerový systém (CCTV) sú rôznorodé. Kamerový systém je inštalovaný v priestoroch administratívnych budov a vybraných objektoch KI. Záznam z týchto kamier sa ukladá lokálne a je možné spätné pozeranie záznamov v prípade incidentu. Žiadny CCTV systém nie je integrovaný do centrálneho dohľadového systému.

Nahrávanie kamier je len lokálne a nedá sa vzdialene sledovať v reálnom čase. Doba nahrávania je taktiež odlišná, záleží od použitej technológie kamier, nahrávacích systémov a pod. Na niektorých objektoch sú inštalované falošné kamery na odstrašenie páchateľa, alebo kamery čo už nefungujú, taktiež plnia účel odstrašenia.

### 2.6.4 Analýza centrálneho softvér pre správu hlášok

Aktuálny software pre správu PZTS a EKV, ktorý spoločnosť využíva, je Advanced building intelligence (ABI). Tento systém je centralizovaný. Pre spoločnosť ABI ho spravuje a servisuje externá spoločnosť, poskytuje vyhradené práva pre správu systému, pričom pracovníci spoločnosti systém využívajú v užívateľskom režime na prezeranie aktuálneho stavu zabezpečenia.

## 2.7 SLEPT analýza

SLEPT analýza sa zameriava na skúmanie jednotlivých oblastí vonkajšieho prostredia spoločnosti a v istých bodoch aj z vyšším zameraním na odvetvie energetiky.

### 2.7.1 Sociálny faktor

V Českej republike dochádza nielen k rastu ekonomiky a životnej úrovne obyvateľov, ale aj k neustálemu zvyšovaniu úrovne požiadaviek na bezpečnosť. Populácia čoraz viac využíva internet na: získavanie informácií, nákupy, vybavovanie agendy a ostatných aktivít prostredníctvom moderných technológií. S rastúcou životnou úrovňou rastie aj nutnosť zabezpečenia systémov pre skvalitnenie ochrany osôb a ich osobných údajov. Obecne vzniká požiadavka pracovníkov na rast miezd, ktorý v prípade nevyhovenia môže zapríčiniť odchod súčasných kvalifikovaných zamestnancov a tým vzniká vyšší dopyt po zamestnancoch.

### 2.7.2 Legislatívny faktor

Na energetickú spoločnosť sa podľa zákonov vzťahuje veľký počet rôznych regulácií, noriem a zákonov. Prvky kritickej infraštruktúry sú určované na základe prierezových a odvetvových kritérií. Kybernetickú bezpečnosť upravujú zákonné piliere ako napr. zákon č. 181/2014 Sb., o kybernetickej bezpečnosti, vyhláška č. 316/2014 Sb., o bezpečnostných opatreniach, kybernetických bezpečnostných incidentoch, reaktívnych opatreniach a o stanovenie náležitostí podania v oblasti kybernetickej bezpečnosti, nariadenie vlády č. 432/2010 Sb., o kritériách pre určenie prvkov kritickej infraštruktúry v znení novely č. 315/2014 Sb., vyhláška č. 317/2014 Sb., o významných informačných systémoch a ich určujúcich kritériách. (6)

Konkrétne požiadavky na zabezpečenie prvku KI špecifikuje norma *ČSN P 73 4450-1*. Ako dodávateľ a distribútor energiou potom tiež spoločnosť podlieha regulácii zo strany Energetického regulačného úradu.

### 2.7.3 Ekonomické faktory

Česká ekonomika v súčasnosti zaznamenáva hospodársky rast, pretože dochádza k rastu domáceho dopytu po produkcii firiem a tým k rastu hrubého domáceho produktu. Na trhu práce sa prejavuje pokles nezamestnanosti, rast príjmov a priemernej mzdy. Avšak ovplyvnenia môžu nastať zo strany regulačného úradu. V aktuálnej dobe sa nepredpokladajú výrazné zmeny. Najzásadnejším ekonomickým faktorom je financovanie daného projektu, ktorý bude hradený zo strany spoločnosti.

### 2.7.4 Politické faktory

V Českej republike je stabilná politická situácia. Súčasná vláda podporuje navýšenie úrovne bezpečnosti najmä pre subjekty KI. Politické rozhodnutia a regulačné inštitúcie ovplyvňujú problematiku riadenia sietí v energetike.

Medzi hlavné činnosti regulácie v sektore energetiky patria:

- tvorba cien elektrickej energie v rámci distribučného reťazca,
- vysoké náklady na budovanie infraštruktúry a distribučné sústavy,
- ekologické limity na výrobu elektrickej energie,
- výroba elektrickej energie z obnoviteľných zdrojov,
- majetkové prepojenie spoločností,
- miera a forma zdanenia činností.

Vyššie uvedené činnosti regulácie taktiež úzko súvisia s ekonomickými a legislatívnymi faktormi celej analýzy a značne ovplyvňujú celkový chod a správanie spoločnosti.

### 2.7.5 Technologický faktor

Inovácia technológií v oblasti zabezpečovacích systémov pre fyzickú bezpečnosť objektov neustále napreduje. Je zaznamenaný neustály technologický vývoj, ktorý vyžaduje nepretržité zlepšovanie znalostí užívateľov, čo tieto systémy využívajú.

Na Českom trhu pôsobia dodávatelia technických prvkov zabezpečenia, informačných systémov na správu a obsluhu zmienených zariadení, alebo komplexní dodávatelia

celého riešenia zabezpečenia. Dodávatelia poskytujú možnosť školení pre interných zamestnancov, aby vykonávali inštalačné práce, pravidelné revízie a kontrolu nad technickým stavom zabezpečovaných systémov. Treba zmieniť, že je nutné získať technické riešenie, ktoré odpovedá požiadavkám normy *ČSN P 73 4450-1*. Zavedením daných technických opatrení spoločnosť zvýši bezpečnosť ochrany majetku a osôb, taktiež plní legislatívne a politické požiadavky.

## 2.8 SWOT analýza

Zostavená SWOT matice spoločnosti celkovo zahŕňa významné slabé a silné stránky, príležitosti a hrozby, plynúce z jej vonkajšieho i vnútorného prostredia. Analýza vychádza z predošlých analýz (7S analýzy, analýzy IS / IT, a SLEPT analýzy) a zameriava sa na spoločnosť, najmä vzhľadom na jej uvažovanej investícii do elektronických zabezpečovacích systémov a evidenciu kontroly vstupu.

Tabuľka 5: SWOT analýza (vlastné spracovanie)

| **SILNÉ STRÁNKY (S)** | **SLABÉ STRÁNKY (W)** |
|---|---|
| • finančná stabilita spoločnosti,<br>• pracovný kolektív na vysokej profesionálnej úrovni,<br>• definované normy a legislatíva,<br>• podpora vedenia spoločnosti,<br>• vysoká kvalita dodávaných služieb. | • sporadicky, nesystematicky zavedené EZS,<br>• financovanie z vlastných zdrojov,<br>- investícia nezvýši potenciálny zisk,<br>• nedostačujúca úroveň zabezpečenia,<br>• nepraktický, nevhodný IS pre správu zabezpečovacích systémov. |
| **PRÍLEŽITOSTI (O)** | **HROZBY (T)** |
| • zvýšenie bezpečnosti v oblasti ochrany majetku a osôb,<br>• zlepšenie kontroly a evidencie pohybu zamestnancov,<br>• verejná prezentácia navýšenia úrovne zabezpečenia, PR,<br>• možnosť získania dotácií na realizáciu,<br>• spolupráca s novými dodávateľmi<br>• nové technologické prostriedky. | • zmeny a nedodržanie legislatívy,<br>• nekvalitné, oneskorené dodanie riešenia dodávateľom,<br>• projektové chyby a nedostatky,<br>- následky: pokuty od dozorného úradu, nefunkčnosť systému,<br>• nedostatok kvalifikovaných pracovníkov v súvislosti s kontinuitou projektu. |

**Záverečné zhrnutie analýz**

Po vykonaní SWOT analýzy možno usúdiť, že pre ďalší rozvoj spoločnosti je vhodná stratégia ST, ktorá predstavuje zníženie hrozieb prostredníctvom využitia silných stránok spoločnosti. V spoločnosti chýba komplexný návrh elektronických zabezpečovacích systémov a evidenciu kontroly vstupu. Návrh obsahuje špecifikáciu technických aspektov EZS a systémov na EKV, centrálny IS pre správu týchto prvkov, školenia interných zamestnancov, implementačné práce apod. Taktiež znížením popisovaných hrozieb nastane využitie príležitostí, ako sú zlepšenie kontroly a evidencie pohybu zamestnancov, ochrana majetku, osôb a iné.

## 2.9 Analýza rizík

Analýza rizík spoločnosti obsahuje identifikáciu a ohodnotenie aktív, identifikáciu hrozieb a zraniteľností a stanovenie miery rizika.

### 2.9.1 Správa rizík

Pre zaistenie celkového úspechu projektu je vhodné vykonať analýzu možných rizík, ktoré by mohli mať vplyv na priebeh a stanovený cieľ celého projektu.

### 2.9.2 Analýza rizík

Pre analýzu rizík bola použitá metóda RIPRAN, pričom nasledujúce tabuľky obsahujú kritériá pre kvantitatívne hodnotenie pravdepodobnosti a dopadu rizík a celkové ohodnotenie závažnosti rizík projektu vrátane slovného popisu.

Tabuľka 6: Hodnotenie pravdepodobnosti rizika (vlastné spracovanie)

| HODNOTA | ČÍSELNÉ VYJADRENIE | SLOVNÉ VYJADRENIE |
|---|---|---|
| 1 | 0 % - 30 % | Nízka pravdepodobnosť |
| 2 | 30 % - 65 % | Stredná pravdepodobnosť |
| 3 | 65 % - 100 % | Vysoká pravdepodobnosť |

Tabuľka 7: Hodnotenie dopadu rizika (vlastné spracovanie)

| HODNOTA | ČÍSELNÉ VYJADRENIE | SLOVNÉ VYJADRENIE |
|---|---|---|
| 1 | Do 20 000 Kč | Zanedbateľný dopad |
| 2 | 21 000 - 95 000 Kč | Ohrozujúci dopad |
| 3 | Nad 95 000 Kč | Kritický dopad |

Tabuľka 8: Celková hodnota závažnosti rizík (vlastné spracovanie)

| Dopad / Pravdepodobnosť | 1 (Do 20 tis. Kč) | 2 (21 tis. - 65 tis. Kč) | 3 (Nad 65 tis. Kč) |
|---|---|---|---|
| 1 (0 % - 30 %) | 1 (Nízka) | 2 (Nízka) | 3 (Stredná) |
| 2 (30 % - 65 %) | 2 (Nízka) | 4 (Stredná) | 6 (Vysoká) |
| 3 (65 % - 100 %) | 3 (Stredná) | 6 (Vysoká) | 9 (Vysoká) |

V nasledujúcej tabuľke sú zobrazené identifikované riziká, ktoré môžu v súvislosti s realizáciou projektu nastať. Pre každú hrozbu je popísaný scenár a podľa uvedených stupníc stanovená pravdepodobnosť (P) výskytu a nepriaznivého dopadu (D) jednotlivých rizík na projekt a na základe ich **súčinu** získaná hodnota rizika (H).

Tabuľka 9: Identifikácia a ohodnotenie možných rizík projektu (vlastné spracovanie)

| ČÍSLO | HROZBA | SCÉNÁR | P | D | H |
|---|---|---|---|---|---|
| **Technologické riziká** | | | | | |
| 1 | Výpadok na vedení z dôvodu poruchy | Prerušenie dodávky elektriny a nefunkčnosť systému | 1 | 3 | 3 |
| 2 | Zlyhanie batérií pre záložný zdroj napájania | Nefunkčnosť redundantného napájania a nefunkčnosť systému | 1 | 3 | 3 |
| 3 | Porucha technických prvkov zabezpečenia | Nefunkčnosť celého systému, alebo jeho jednotlivých častí | 2 | 2 | 4 |
| 4 | Porucha kabeláže | Prerušenie komunikácie prvkov | 1 | 2 | 2 |
| **Procesné riziká** | | | | | |
| 5 | Nedostatočné preškolenie pracovníkov | Nesprávne fungujúci systém, nefunkčnosť systému | 2 | 3 | 6 |
| 6 | Podcenená analýza software | Nevhodne stanovené požiadavky na software | 1 | 3 | 4 |
| 7 | Chýbajúca funkcionalita prvkov systému | Nedostatočné zabezpečenie, nekompatibilita systému | 1 | 3 | 4 |
| **Bezpečnostné riziká** | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| 8 | Nedostatočné zabezpečenie software pre správu systému | Neoprávnený vstup do systému, únik dát, narušenie dostupnosti systému | 2 | 3 | 6 |
| 9 | Falšovanie užívateľskej identity cudzími osobami | Zneužitie, znehodnotenie, nefunkčnosť systému | 2 | 3 | 6 |
| 10 | Nedostatočné zabezpečenie komunikácie medzi prvkami | Zneužitie zraniteľnosti prvkov všeobecne, nefunkčnosť systému | 2 | 3 | 6 |
| **Riziká fyzického charakteru** | | | | | |
| 11 | Zničenie bezpečnostných prvkov | Vyradenie funkčnosti celého systému | 2 | 3 | 6 |
| 12 | Krádež vykonaná cudzími osobami | Vyradenie funkčnosti celého systému | 2 | 2 | 4 |
| 13 | Krádež vykonaná pracovníkmi tretích strán | Vyradenie funkčnosti celého systému | 2 | 2 | 4 |
| **Organizačné riziká** | | | | | |
| 14 | Nedodržanie pracovných postupov | Spôsobenie škody na majetku a zdraví | 1 | 2 | 2 |
| 15 | Nedodržanie termínu zo strany dodávateľa | Predĺženie termínu projektu, hroziace sankcie z kontrolných úradov | 3 | 3 | 9 |
| 16 | Nedostatočné zmluvné zabezpečenie | Neposkytnutie náležitých služieb | 2 | 3 | 6 |
| **Finančné riziká** | | | | | |
| 17 | Neočakávané dodatočné náklady | Navýšenie celkového rozpočtu na projekt | 2 | 3 | 6 |

V uvedených kategóriách rizík bolo celkovo identifikovaných a ohodnotených 17 rizík projektu, pričom 8 s vysokou hodnotou, 7 so strednou a 2 s nízkou hodnotou rizika.

Tabuľka nižšie uvádza návrhy na opatrenia na zníženie hodnoty jednotlivých rizík a v stĺpcoch P, D a H už znížené hodnoty po implementácii opatrení.

Tabuľka 10: Návrhy na opatrenia identifikovaných rizík projektu (vlastné spracovanie)

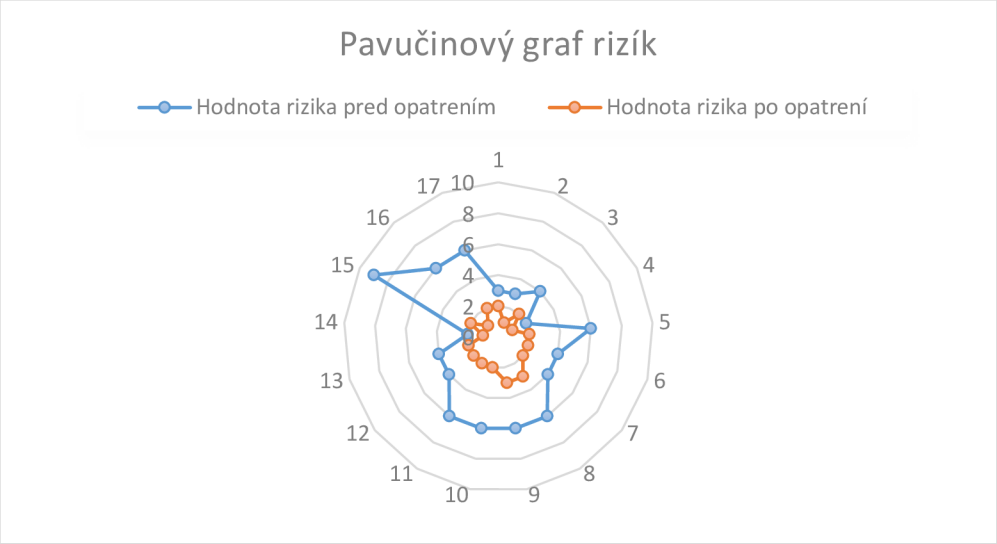
| ČÍSLO | NÁVRHY OPATRENÍ | P | D | H |
|---|---|---|---|---|
| **Technologické riziká** | | | | |
| 1 | Zaistenie redundantného zdroja napájania, záložné zdroje | 1 | 2 | 2 |
| 2 | Pravidelné kontroly a revízie batérií | 1 | 1 | 1 |
| 3 | Pravidelné revízie, výmena zariadenia po dobe záruky | 1 | 2 | 2 |
| 4 | Výber dôveryhodného dodávateľa, certifikácia a záruka kabeláže | 1 | 1 | 1 |
| **Procesné riziká** | | | | |
| 5 | Dôsledný plán školení, priestor pre dotazy, praktický tréning | 1 | 2 | 2 |
| 6 | Dôkladná analýza potrebnej funkcionality, externé poradenstvo | 1 | 2 | 2 |
| 7 | Zadefinovanie funkcií na základe analýzy procesov, testovanie demo verzií | 1 | 2 | 2 |

| | | | | |
|---|---|---|---|---|
| **Bezpečnostní riziká** | | | | |
| 8 | Zistiť úroveň bezpečnosti informácií daného IS, zohľadniť úroveň pri výbere IS, stanovenie zodpovednosti v zmluvnom vzťahu | 1 | 3 | 3 |
| 9 | Precízne preškolenie zamestnancov, sankcie za porušovanie pravidiel | 1 | 3 | 3 |
| 10 | Zistiť úroveň bezpečnosti prvkov, zohľadniť úroveň pri výbere prvkov, testovanie prvkov v demo sieti, nastavenie pravidiel pre prácu s prvkami | 1 | 2 | 2 |
| **Riziká fyzického charakteru** | | | | |
| 11 | Znemožnenie voľného prístupu k prvkom, umiestnenie prvkov v bezpečnej výške, informovanie lokálnej polície o možnosti vandalizmu, vyznačenie informačných tabuliek | 1 | 2 | 2 |
| 12 | Znemožnenie voľného prístupu k prvkom, umiestnenie prvkov v bezpečnej výške, informovanie lokálnej polície o možnosti vandalizmu, vyznačenie informačných tabuliek, forenzné značenie | 1 | 2 | 2 |
| 13 | Stanovenie zodpovednosti v zmluvnom vzťahu, vyznačenie informačných tabuliek, forenzné značenie | 1 | 2 | 2 |
| **Organizačné riziká** | | | | |
| 14 | Preškolenie zamestnancov, stanovenie zodpovednosti v zmluvnom vzťahu, sankcie | 1 | 1 | 1 |
| 15 | Kontrola harmonogramu, časové rezervy, prípadné zmluvné zaistenie | 1 | 2 | 2 |
| 16 | Analýza zmluvy, stanovení zodpovednosti, garancie služby a stanovenie sankcií, prípadne vyjednanie lepších podmienok | 1 | 1 | 1 |
| **Finančné riziká** | | | | |
| 17 | Podrobne vykonaná kalkulácia rozpočtu, finančné rezervy | 2 | 1 | 2 |

Implementáciou daných opatrení sa hodnota akýchkoľvek rizík zníži aspoň o jednu úroveň, takmer všetky riziká sú ohodnotené ako nízka úroveň, iba riziko č. 8 a 9 je hodnotené ako stredná úroveň. So zavedením určitých opatrení sú spojené finančné náklady (napr. na školenia či implementačné služby dodávateľa), ktoré sú zahrnuté v ekonomickom zhodnotení. Ostatné opatrenia majú formu odporúčaní a nevyžadujú žiadnu investíciu.

### 2.9.3 Mapa rizík

Nasledujúci graf zobrazuje mapu rizík pomocou pavúčieho grafu, kde fialová čiara vyjadruje hodnotu všetkých 17 identifikovaných rizík pred implementáciou opatrenia a zelená čiara predstavuje zníženú hodnotu rizík po zavedení navrhovaných opatrení.




Obrázok 2: Pavučinový graf rizík projektu (vlastné spracovanie)

# 3 VLASTNÉ NÁVRHY RIEŠENIA

V tejto kapitole sa práca bude venovať návrhu požiadaviek na dodávateľa elektronických zabezpečovacích systémov pre objekty KI v spoločnosti. Budú popísané potrebné technické parametre a funkcionality zo všeobecného hľadiska a následne pre konkrétne prvky zabezpečovacích systémov tak, aby splňovali normu ČSN P 73 4450-1, všetky legislatívne a interné požiadavky. Záverom kapitoly bude tento všeobecný návrh aplikovaný na konkrétny objekt, pre účel zistenia aplikovateľnosti.

## 3.1 Všeobecné technické požiadavky

Všetky prvky STO ako sú detektory, snímače, kamery, reflektory, klávesnice, ovládače, hlavy čítačiek kariet, magnety a pod. Musia svojimi parametrami vyhovovať pre nasadenie v danom prostredí. Pod parametrami sa rozumejú rozsahy prevádzkových teplôt (vonkajšie priestory -25 °C až +55 °C, vnútorné priestory: +5 °C až + 40°C), krytie (vonkajšie priestory IP44 a vnútorné priestory IP21), odolnosť (záleží na špecifických okolnostiach) a iné. V prípade nasadenia v prostredí s nebezpečenstvom výbuchu, alebo inom rizikovom prostredí tomu podobnom musí dodávateľ, resp. zhotoviteľ, doložiť všetky potrebné certifikáty o spôsobilosti prvkov a kvalite inštalačnej práce.

Dodávané prvky STO musia byť voľne distribuované na trhu v Českej republike, alebo musia mať aspoň dodávateľské zastúpenie, čo zabezpečí technickú podporu vrátane školenia pre inštaláciu, obsluhu a servis po dobu najmenej 10 rokov od zavedenia systému do prevádzky.

Medzi požiadavky sa taktiež radí maximálne možné využitie existujúcej inštalovanej infraštruktúry, prvkov STO a napájacích systémov, ktoré vlastní spoločnosť. Ide o integráciu stavajúcich systémov, ktorá bude bližšie popísaná pri konkrétnych prvkoch zabezpečenia.

Dodaný software pre dohľadové a prijímacie poplachové centrum (DPPC) musí taktiež umožňovať integráciu existujúcich systémov PZTS a VSS. V prípade požiadavky na

integráciu spoločnosť zaistí súčinnosť vo forme odovzdania popisu použitého rozhrania využívaných komunikačných protokolov, parametrov a technických dokumentácií pre uskutočnenie integrácie.

Nové dodané systémy PZTS a VSS musia disponovať možnosťou prispôsobenia sa prostrediu, procesom, pravidlám a hlavne napojeniu sa na existujúcu infraštruktúru a zaistiť tak chod celkového systému bez problémov s kompatibilitou.

## 3.2 Prvky požiarnych zabezpečovacích a tiesňových systémov

Všetky prvky PZTS **vrátane inštalačných prác dodávateľa** musia spĺňať stupeň zabezpečenia 3 podľa ČSN EN radu 50 131-1 ed.2, nakoľko túto úroveň zabezpečenia vyžaduje norma ČSN P 73 4450-1.

### 3.2.1 Ústredňa PZTS

Ústredňa PZTS musí byť dynamicky škálovateľná s možnosťou budúceho rozširovania, alebo doplňovania v každom inštalovanom objekte – modulárne riešenie. Rozšírenie znamená možnosť budúceho pridávania prvkov (modulov) bez obmedzení, zmeny jadra, pričom musí byť zachovaný typ a verzie ústredne PZTS pre správny chod systémov. Odporúčam plánovať aspoň s 30% rezervou oproti reálnemu počtu zariadení.

Pri realizácií odporúčam použiť proprietálny systém PZTS (ústredňa, napájanie, klávesnica pre manažment, systémové a riadiace moduly) od jedného výrobcu, ktorý dokáže garantovať stanovené podmienky, ako sú modulárnosť či kompatibilita.

Medzi funkcie ústredne PZTS musí patriť manažment modulov pre snímanie bezkontaktných kariet, vrátane pripojenia do jednotnej databázy používateľov spravovanej na DPPC. Ústredňa PZTS musí vedieť obslúžiť minimálne 32 rôznych oprávnení prístupu – subsystémov objektu tak, ako to určuje norma.

Kapacita pamäte ústredne PZTS musí byť dimenzovaná aspoň na 1024 udalostí zo snímačov a prvkov PZTS, samostatnú pamäť pre záznam prístupov (vstupov / výstupov) cez čítačky kariet a pamäť lokálnej databázy užívateľov minimálne 1024 záznamov.

Ďalej musí ústredňa PZTS vedieť obslúžiť (zaznamenávať, prípadne vyhodnotiť signály) 250 prvkov PZTS, a konfigurovať a spravovať 32 subsystémov.

U objektov s požadovanou nižšou úrovňou zabezpečenia (kategória III) môže byť navrhnutý nižší model ústredne rovnakej modelovej rady. Podmienkou je využívanie rovnakých systémových modulov a možnosť rozšírenia kapacity a to pridaním ďalších modulov.

Kapacita záložných akumulátorových zdrojov musí byť dimenzovaná na minimálne 4 hodiny prevádzky podľa normy ČSN EN 50131.

Konfigurácia ústredne musí byť prístupná lokálne priamo na displeji konfiguračného rozhrania, no výhodou je, ak je tam možnosť aj vzdialeného prístupu, avšak s touto možnosťou plynú riziká zneužitia. Ak by sa táto požiadavka naskytla, odporúčam preveriť bezpečnostné protokoly pre vzdialený prístup.

Ústredňa PZTS musí vedieť komunikovať s DPPC, musí obsahovať rozhranie LAN, pre zabezpečené funkcie ako je: on-line monitoring všetkých systémových stavov (stav stráženia / odblokovanie), poplachov a porúch v sledovanom systéme či aktuálny stav konkrétnych prvkov zabezpečenia.

Ak dôjde k výpadku komunikácie medzi ústredňou PZTS a centrálnym dohľadovým systémom (software), systém bude pokračovať bez zmeny. Nesmie nastať obmedzenie funkcií a činnosti celého zabezpečenia. Databáza užívateľov v lokálnej pamäti využíva posledný aktuálny zoznam a po opätovnom naviazaní komunikácie si musí túto databázu aktualizovať z centrálnej databázy.

Taktiež musí umožňovať dátové pripojenie certifikovaného poplašného prenosového systému podľa ČSN EN 50136-1, zabezpečujúceho prenos podrobných a adresných poplachových a prevádzkových informácií na DPPC. PZTS musí umožňovať automatické zamietnutie prístupu v prípade, že daný vstup odošle počas nadefinovaného časového obdobia určitý počet (falošných) poplachov. Zamietnutý vstup sa spätne aktivuje „resetom“ (klávesnicou alebo na diaľku z DPPC), alebo automaticky, ak nedetekuje falošné poplachy po určenú nadefinovanú dobu.

### 3.2.2 Snímače prístupových kariet

Pre zabezpečenie kompatibility s aktuálnymi systémami je nutné, aby hlava čítačky kariet podporovala rozhranie Wiegand, nakoľko inštalované ústredne PZTS podporujú práve toto rozhranie. V tomto prípade nie je nutné, aby hlavy boli od jedného výrobcu, ale aby podporovali toto rozhranie.

Moduly pre snímanie kariet musia obsahovať funkciu pre riadenie prístupu, vrátane ovládania elektrických dverí (odomknúť / zamknúť), tiež funkciu zablokovania / odblokovania prístupu jedného, alebo rôznych subsystémov objektu.

Moduly ďalej musia vedieť komunikovať s ústredňou PZTS po priložení karty na hlavu čítačky kariet. Autentizáciu a autorizáciu bude vykonávať ústredňa PZTS zo svojej lokálnej databázy. Danú databázu musí pravidelne aktualizovať, komunikáciou s centrálnou databázou, umiestnenou na DPPC.

Snímacie hlavy musia jednoznačne a jednoducho signalizovať aktuálny stav zabezpečenia. V prípade ovládania viacerých subsystémov z jedného snímača, musí byť stav každého stavu zvlášť vyznačený, aby bolo jasné s akým subsystémom sa manipuluje.

### 3.2.3 Detektory a snímače PZTS

Táto časť popisuje technické parametre, ktoré musia prvky zabezpečenia spĺňať tak, aby boli splnené požiadavky normy ČSN P 73 4450-1.

**Duálny detektor pohybu:**

- minimálne dva rozličné detekčné princípy snímania pohybu, kvôli presnejšiemu vyhodnoteniu situácie a minimalizácií falošných poplachov,
- možnosť sériového zapojenia minimálne 5 detektorov za sebou,
- digitálne vyhodnotenie signálu,
- doba trvania vyhodnotenia situácie maximálne 300 milisekúnd,
- plynule nastaviteľná citlivosť a dosah mikrovlnných častí,

- najmenej 3 rôzne frekvencie mikrovlnných časti - možnosť inštalácie viac detektorov vo svojej blízkosti bez vzájomného rušenia,
- možnosť inštalácie na stenu alebo strop,
- dosah snímacieho záberu minimálne 12 m a rozsah 90°.

**Detektor hluku a rozbitia skla:**

- dosah snímania zvuku minimálne 7 m,
- nastavenie minimálne 3 rôznych úrovní citlivosti v decibeloch,
- detekcia rozbitia pre všetky typy skiel, vrátane drôteného, tvrdeného, vrstveného, lepeného skla a skla s bezpečnostnou fóliou,
- možnosť inštalácie na stenu alebo strop,
- digitálne vyhodnotenie signálu.

**Magnetický kontakt:**

- prispôsobené pre montáž na podkladový materiál (drevo, plast, kov),
- dosah snímania minimálne 1 cm,
- variabilný tvar pre špeciálne umiestnenie,
- vedenie vodičov signálu v ochrannej lište.

V prípade umiestenia magnetických kontaktov na pojazdné brány, bránky, garážové dvere a pod. je nutné, aby boli splnené požiadavky:

- povrchová montáž pre podkladový materiál na feromagnetické povrchy,
- vyvedenie vodičov signálu pancierovou vývodkou,
- dosah snímania minimálne 3 cm.

**Kompatibilita systémov:**

Súčasné prvky, ktoré nevyhovujú požiadavkám stupňu zabezpečenia 3 podľa ČSN EN radu 50 131-1 ed.2, budú nahradené novými.

V prípade, že prvky splňujú daný stupeň zabezpečenia 3, dodávateľ musí zaistiť dodanie takých prvkov, ktoré sú kompatibilné s inštalovanými prvkami, vrátane

bezproblémovej komunikácie s ústredňou PZTS, na základe používaných komunikačných protokolov.

Pod požiadavkami kompatibility si možno predstaviť:

- synchronizácia času prvkov PZTS podľa času servera,
- výmena informácií, všetkých prevádzkových stavov a adries detektorov v rámci bezpečnostných zón a systémových prvkov, medzi ústredňou a jednotlivými prvkami PZTS,
- možnosť sériového zapojenia prvkov s jednoznačnou adresáciou prvku v sieti,
- ovládanie výstupných brán a dverí formou impulzu po definovaný čas, alebo formou trvalej aktivácie (do najbližšej zmeny stavu),
- vzájomná kompatibilita čítačiek vstupných kariet a komunikácia s databázou užívateľov (povolenie / odmietnutie prístupu).

## 3.3 Prvky dohľadových videosystémov

Všetky prvky VSS **vrátane inštalačných prác dodávateľa** musia byť certifikované podľa stupňa zabezpečenia 3 podľa ČSN EN radu 62676-1-1, nakoľko túto úroveň zabezpečenia vyžaduje norma ČSN P 73 4450-1.

VSS systém musí byť navrhnutý tak, aby bol schopný pripojiť, spravovať a monitorovať (v konečnom stave) najmenej 150 objektov a 1500 kamier.

V prípade inštalácie kamier na komunikačných trasách (prístupové komunikácie vo vnútri objektu, chodby, a pod.) je nutné, aby kamery plnili funkcionalitu pozorovania (zameranie na charakteristické detaily jednotlivca) a súčasne umožňovali sledovanie aktivity v okolí.

### 3.3.1 Záznamové zariadenie

Záznamové zariadenie bude umiestnené v každom objekte KI a bude splňovať nasledujúce požiadavky:

- rozšíriteľnosť- zariadenie musí umožňovať postupné pridávanie a doplňanie výbavy podľa potreby, najmä v oblasti pridávania počtu kamier, zvyšovania celkovej dátovej priepustnosti a diskovej kapacity,
- pri plnom vyťažení musí zariadenie zaistiť dostatočnú dátovú priepustnosť a disponovať dostatočným výkonom pre záznam všetkých kamier rýchlosťou 25 snímok za sekundu (fps) v maximálnej kvalite a rozlíšení Full HD (1080p),
- v prípade potreby, musí umožňovať zobrazenie všetkých zapojených kamier prostredníctvom LAN pre pracovníkov DPPC:
  a) vzdialene - 2 monitory so zobrazením 1 až 16 kamier v plnej snímkovej rýchlosti,
  b) lokálne - 1 až všetkých kamier, pre občasný monitoring a na servisné účely, zobrazenie.
- minimálne gigabitové sieťové rozhranie s podporou komunikačných protokolov TCP/IP, DHCP, DNS, NTP, SMTP, SNMP, HTTPs, IPv6,
- podpora video-analytických funkcií (v spojení s vybranými kamerami) až pre maximálny počet vstupov,
- zapojenie HD kamier do záznamového zariadenia musí využívať prenos signálu bez využitia IP siete, a to použitím HDTV a pod.,
- možnosť pripojenia minimálne dvoch vysokokapacitných harddiskov a nastavenie redundantného ukladania záznamu,
- možnosť dvoch dátových streamov, rôzneho nastavenia pre záznam a pre zobrazenie,
- prepojenie s ústredňou PZTS,
- spätné prehrávanie situácií pri spustení poplachu PZTS pomocou vložených časových značiek, inteligentné vyhľadávanie v zázname podľa pohybu vo vybranej časti objektu, alebo narušení zóny,
- možnosť synchrónneho prenosu všetkých pripojených kamier,

Požiadavky na možnosti a kvalitu záznamu:

- doba trvania záznamu minimálne 30 dní v celkom rozsahu záznamu, pre všetky zariadenia zapojené v systéme.

- alarmový záznam - rýchlosť snímania 25 fps , režim snímania sa spustí pri vyhlásení poplachu, alebo vzdialeným spustením. Koniec nahrávania nastane 30 sek. po ukončení poplašného stavu,
- stály záznam - rýchlosť snímania 3 - 12 fps,
- export záznamu lokálne cez USB.
- možnosť nastavenia individuálneho diskového priestoru pre každú kameru.

### 3.3.2 Videomanažment záznamového zariadenia

V kapitole sú spísané požiadavky na funkcionalitu software pre systém video-manažment (VMS), inštalovaného na lokálnych PC a vzdialených staniciach DPPC.

Software pre VMS musí byť dodaný v plnej verzií (pre DPPC) a môže byť aj v odľahčenej verzií. Odľahčená verzia bude inštalovaná na lokálnych staniciach, dané stanice nevyžadujú plnú funkcionalitu, ale slúžia len na prístup k živému obrazu, alebo záznamu, podľa pridelených prístupových práv.

**Plná verzia software**

Plná verzia software musí splňovať nasledujúce požiadavky:

- verzia softwaru musí podporovať inštaláciu na bežne dostupné komerčné operačné systémy, bez vynútenej licencie na neobmedzený počet staníc v českom jazyku,
- možnosť zobrazenia kamier z rôznych zariadení súčasne na jednom monitore klientskej stanice a integrované mapové rozhranie - možnosť umiestnenia aktívnych symbolov kamier do máp (zobrazenie stavu kamery),
- kompletná správa celého systému (kamery, disky, klientske stanice, užívateľské kontá a pod.)
- podpora zobrazenia a správy panoramatických a hemisférických kamier,
- možnosť definície užívateľov, užívateľských práv pre správu záznamu, zobrazenia a činností s tým spojených,
- možnosť definície vlastných užívateľských vizuálnych rozhraní s pohľadmi kamier,

- možnosť ovládania kamier joystickom, alebo myšou na obrazovke,
- možnosť nastavenia zasielania automatických upozornení, poplachových správ a informácií na predvolené e-mailové adresy, príp. SMS cez globálny systém mobilnej komunikácie (GSM)
- komplexný denník udalostí ukladaním všetkých prevádzkových udalostí, alarmov, porúch a užívateľských akcií, možnosti zobrazenia vybraných kategórií udalostí, možnosť vkladania užívateľských poznámok, možnosť filtrácie a vyhľadávanie podľa časovej značky a podľa kategórií.

### 3.3.3 Kamery a prvky VSS

**Všeobecné požiadavky pre kamery :**

- HD kamera s podporou prenosu dát cez UTP / FTP kábel bez využitia IP protokolu,
- podpora kodeku H.265, alebo H.264+ (kodek slúži na kompresiu dát a zníženie dátového toku),
- detekcia pohybu, detekcia poruchy, výpadku, zakrytie aj natočenie kamery, prenos do VMS a do centrálneho software DPPC s rozlíšením typu udalosti,
- automatický IR cut filter (dokáže rozoznať a snímať pohyb aj v tme),
- škála širokého dynamického rozsahu - wide dynamic range (WDR) musí byť minimálne 100 decibelov (WDR poskytuje jasný obraz aj za situácie, keď je príliš veľký rozdiel medzi najsvetlejšou a najtmavšou časťou obrazu).

**Kamery pre vnútorné použitie:**

- šírka záberu objektívu 40° až 110°, pri celkovej šírke záberu minimálne 5 m a dĺžke záberu 15 m,
- stupeň ochrany krytím IP21, dizajn krytia DOME alebo BALL,
- integrovaný IR cut filter, s možnosťou demontáže,
- v prípade 360°kamery, možnosť pohybu obrazu v živom prenose aj v zázname pomocou joysticku,
- všeobecné požiadavky pre kamery (popis vyššie).

**Kamery pre vonkajšie použitie:**

- objektív veľkosti 28 mm alebo väčší, rozlíšenie obrazu 2 megapixely pri 25 snímkach za sekundu,
- šírka záberu objektívu 10° až 40°, celková šírka a dĺžka záberu závisí od miesta inštalácie a priestoru, ktorý bude kamera snímať, avšak minimálna šírka záberu 8 m a dĺžka záberu 20 m,
- stupeň ochrany krytím IP66,
- video-analytické autonómne funkcie pre detekciu pohybu a elimináciu falošných poplachov vplyvom vonkajšieho prostredia (poveternostné podmienky, nadmerný hluk v blízkosti objektu a pod.),
- možnosť uchytenia na stenu, príp. na stĺp,
- všeobecné požiadavky pre kamery (popis vyššie).

**Otočné (PTZ) kamery:**

- 30x optický zoom, clona automatická i manuálna,
- Podpora protokolov TCP/IP, ICMP, HTTP, HTTPs, FTP, DHCP, DNS, DDNS, RTP, RTSP, RTCP, NTP, SMTP,
- 360° kontinuálna rotácia, nastaviteľná rýchlosť otáčania (minimálna rýchlosť 60° za sek.), náklon -20° až +115°,
- minimálne 100 predvolieb pohybu, pamäť pre 4 trasy s dĺžkou 5 min.,
- nastavenie izbovej polohy pri nečinnosti,
- integrovaný adaptívne IR prísvit s dosahom 100 m,
- všeobecné požiadavky pre kamery (popis vyššie).

## 3.4 Dohľadový systém

Nasledujúca časť popisuje požiadavky na software a hardware pre dohľadové a poplachové prijímacie centrum. Ďalej obsahuje popis užívateľského rozhrania, jeho funkcionalitu, potrebné funkčné väzby na zabezpečovacie systémy a pod.

### 3.4.1 Požiadavky na vlastnosti systému:

- dohľadový SW musí byť schopný pripojiť a spravovať najmenej 500 prvkov STO (ústrední PZTS, rekordérov VSS, switchov a pod.) A celkovo najmenej 10.000 konkrétnych prvkov (snímačov, kamier, senzorov, čítačiek kariet a pod.)
- hardware musí byť dimenzovaný tak, aby fungovalo plynulé, bezporuchové spracovanie daných informácií,
- dohľadový SW musí mať súčasne dostatočnú kapacitu pre prácu s jednotnou databázou užívateľov (všetci kmeňoví aj externí zamestnanci, dodávatelia tretích strán, návštevnícke karty apod.),
- možnosť fungovania v redundantnom režime v reálnom čase, pri výpadku jednej centrály DPPC ju plne nahrádza ďalšia, maximálna prípustná doba rekonfigurácie je 500 milisekúnd,
- možnosť inštalácie viac serverov so vzájomnou synchronizáciou databáz, ručné aj automatické eskalácie udalostí na vopred definovaný hlavný alebo záložný server,
- funkčné väzby VSS s ďalšími systémami STO,
- záznam činnosti obsluhy DPPC - dátum a čas doručenia udalosti do systému, dátum a čas vzniku udalosti na pripojenom objekte, reakčný čas a spôsob reakcie obsluhy (prijatie udalosti, vyhodnotenie udalosti, uzatvorenie udalosti),
- škálovateľná konfigurácia oprávnení klientskych účtov.

### 3.4.2 Požiadavky na klientsky software:

- Zobrazenie adresnej siete umiestených kamier v jednotlivých objektov (najlepšie vizuálne rozmiestnenie, zakreslené v pôdoryse objektu),
- Jednoduchý intuitívny vzhľad v českom jazyku,
- pri poplachovej udalosti - veľké vizuálne upozornenie, o ktorý objekt a typ narušenia sa jedná a presné inštrukcie, ako ďalej postupovať,
- software musí umožňovať vymedzenie administratívnych a užívateľských práv prístupu k obsluhe klienta, nesmie umožňovať mazanie akýchkoľvek udalostí v histórii bez vykonania záznamu o takomto úkone s identifikáciou, kto a kedy také mazanie vykonal,
- 3 úrovne užívateľov:

- administrátor – správca celého systému, všetky plné práva,
- správca kritickej infraštruktúry – správca prístupov a užívateľských účtov, všetky plné práva vo vymenovanej oblasti 14,
- užívateľ – pracovník DPPC, obmedzené práva podľa situácie.

## 3.5 Modelový objekt

Modelový objekt bol zvolený na základe požiadaviek energetickej spoločnosti, aby demonštroval uplatnenie nasadenia EZS v praxi na reálnom objekte. Podľa tohto modelu budú nasadené EZS aj do ostatných objektov KI spoločnosť, čo predstavuje dohromady približne 120 objektov.

### 3.5.1 Poplašné zabezpečovacie a tiesňové systémy

Ústredňa a celý systém budú mať dostatočnú kapacitu pre prípadné budúce rozšírenie:

- doplnenie snímačov kariet na všetky vonkajšie aj vnútorné dvere,
- rozdelenie na najmenej 4 ďalšie subsystémy.

V rámci plášťovej ochrany objektov budú na vybraných oknách, dverách a vrátach inštalované magnetické kontakty a detektory rozbitia skla. V rámci priestorovej ochrany budú do vybraných miestností inštalované detektory pohybu.

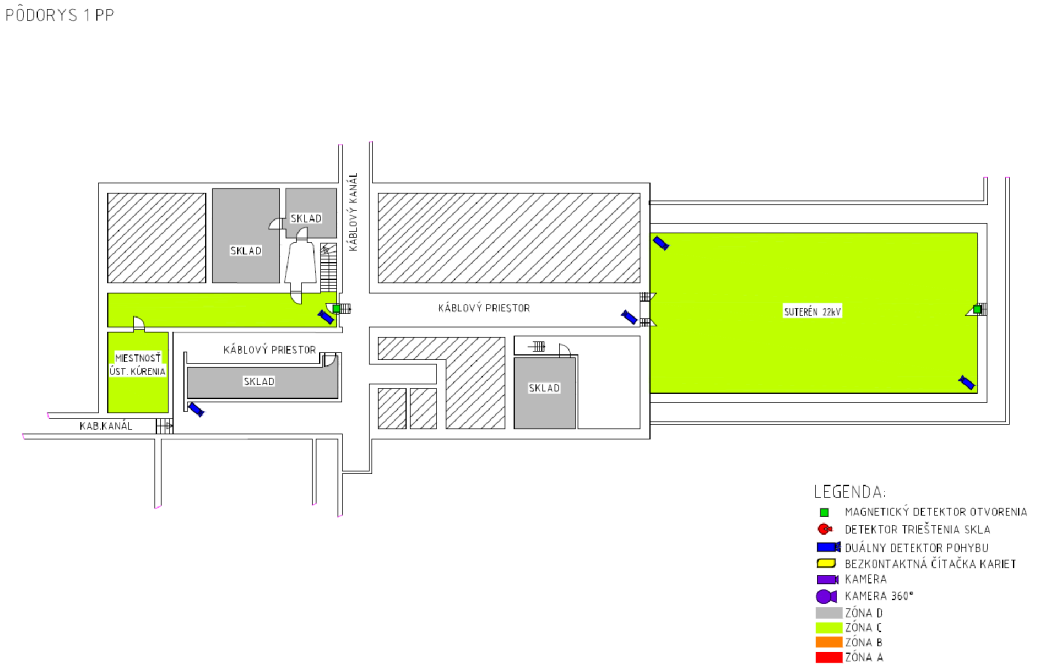
Riadenie prístupu osôb do areálu aj do budovy bude súčasťou systému PZTS. Ústredňa PZTS bude vyhodnocovať oprávnenia prístupu držiteľov identifikačných kariet. V pamäti ústredne PZTS bude uložená história priechodov.

V rámci plášťovej ochrany objektov budú inštalované:

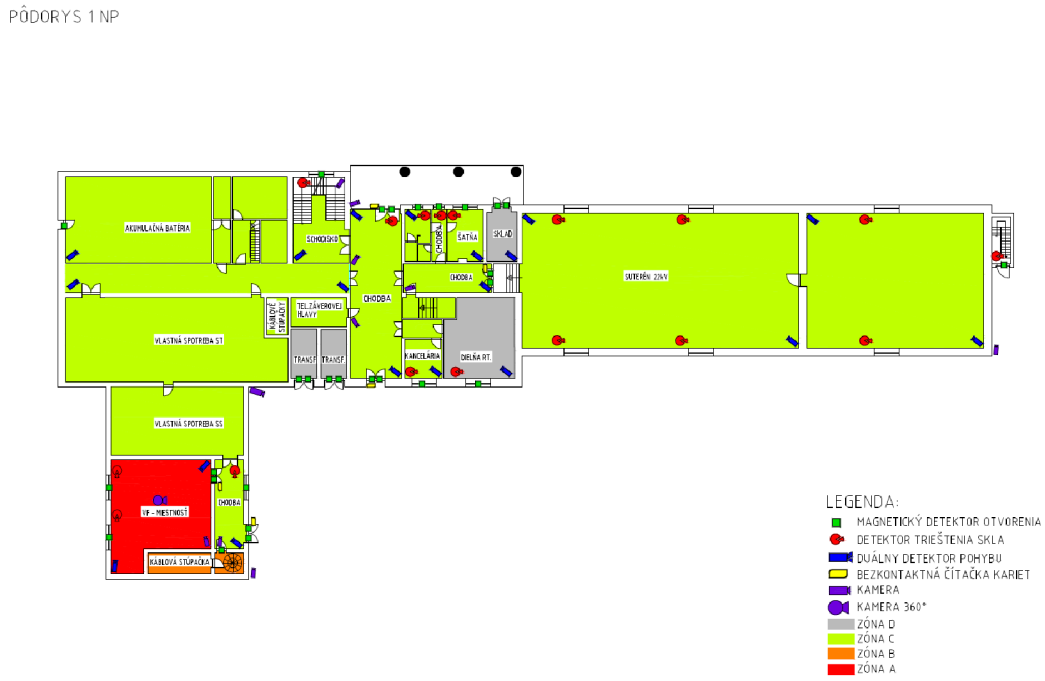
- magnetické kontakty:
  - na všetkých dverách, vrátach,
  - na všetkých oknách prvého nadzemného podlažia budovy,
  - na všetkých vnútorných dverách, riadených snímačmi kariet a opatrených elektromechanickými zámky,
  - na dátovom rozvádzači STO,

- detektory rozbitia skla:
    - vo všetkých miestnostiach s oknami,
- detektory pohybu:
    - do všetkých miestností a chodieb, ktoré aspoň 1 stenou tvoria plášť budovy.

Nasledujúce obrázky vizuálne znázorňujú rozmiestnenie prvkov PZTS a VSS v objekte. Pre detailnejší pohľad na situáciu pôdorysov slúžia prílohy č.1 až 4.




Obrázok 3: Pôdorys 1. podzemného podlažia (príloha č.1)




Obrázok 4: Pôdorys 1. nadzemného podlažia (príloha č.2)


Obrázok 5: Pôdorys 2. nadzemného podlažia (príloha č.3)


Obrázok 6: Pôdorys 3. nadzemného podlažia (príloha č.4)

Vzhľadom k charakteru priestorov sú všetky detektory pohybu navrhnuté v kombinovanom (duálnom) prevedení s pasívnou infračervenou detekciou a súčasne mikrovlnnou detekciou, a to pre maximálnu elimináciu falošných poplachov vplyvom prostredia (prúdenie vzduchu, spúšťanie ventilácie, klimatizácie apod.).

**Ovládanie PZTS**

Ovládanie sa bude prednostne uskutočňovať bezkontaktnou identifikačnou kartou. Stav odkódovania alebo stráženia bude signalizovaný optickou signalizáciou LED na čítačke.

Pri dverách vybavených elektromechanickým zámkom bude snímač kariet súčasne zabezpečovať riadenie vstupu do vnútorného priestoru. Systém odblokuje zámok a kľučku a umožní priechod po priložení platnej karty s oprávnením vstupu.

V prípade, že vnútorný subsystém je v stave stráženia, musí osoba priložiť kartu opakovane. Prvým priložením dôjde najprv k odkódovaniu subsystému, ďalším

priložením potom k odblokovaniu zámku a kľučky. Odchod opačným smerom je možný pomocou kľučky dverí a nie je nijako regulovaný.

Odkódovanie vrátane sledovania stavu jednotlivých subsystémov PZTS bude možné z ovládacej klávesnice s LCD displejom. Pre lepšiu prehľadnosť bude vedľa klávesnice inštalované LED tablo, ktoré signalizuje odlišnými farbami stavy jednotlivých subsystémov.

Výstupom z PZTS bude prepojenie na systém VSS pre aktiváciu kamier a záznamového systému. V prípade spustenia poplachu prvkami PZTS sa automaticky spustí nahrávanie:

- u vnútorných kamier pri poplachu v danom subsystému,
- u vonkajších kamier pri poplachu v danej zóne perimetrického detekčného systému.

**Subsystémy a zóny objektu**

Koncové prvky PZTS budú rozdelené do samostatne ovládaných subsystémov. Návrh rozdelenia PZTS do subsystémov:

- subsystém 1 - vjazdová brána a vstupná bránka,
- subsystém 2 - spoločné priestory vo vstupnej časti budovy a kancelárske priestory,
- subsystém 3 - rozvodňa R 22kV,
- subsystém 4 - klimatizačná miestnosť,
- subsystém 5 - komunikačná miestnosť,
- subsystém 6 - VF miestnosť a telefónna ústredňa,
- subsystém 7 - dozorňa.

Subsystém 1 bude naprogramovaný ako závislý. Pri vstupe cez bránu alebo bránku bude spustená „príchodová procedúra“ a do uplynutia 3 minút musí užívateľ odkódovať akýkoľvek subsystém pomocou klávesnice alebo karty, v opačnom prípade bude spustené poplašné hlásenie na DPPC.

**Signalizácia stavu**

Indikácia stavov PZTS bude vyvedená:

- lokálne:
  - na ovládacej klávesnici PZTS,
  - vo vybraných prípadoch na akustické signalizačné zariadenie,
- diaľkovo:
  - na DPPC centrum prostredníctvom dátového prepojenia,
  - na určené telefónne čísla zamestnancov formou SMS správ a volania, prostredníctvom GSM komunikátora.

Signalizácia stavu subsystému na snímači kariet:

- strážená oblasť je signalizovaná červenou LED diódou,
- načítanie a autentifikácia karty je signalizovaná zelenou LED diódou,
- pri odkódovaní nesvieti žiadna LED dióda.

**Spôsob a umiestnenie prvkov PZTS**

Detektory a snímače kariet v priestore brány a bránky budú zapojené do vonkajšieho rozvádzača, umiestneného v blízkosti brány. Pre zaistenie spoľahlivej komunikácie medzi riadiacimi jednotkami a vzdialenými snímačmi kariet (u vjazdovej brány) je nutné dodržať limity použitého rozhrania. Rozhranie Wiegand je možné prenášať na vzdialenosti maximálne 100 metrov.

Pri každom snímači kariet, ktorý je umiestnený vo vonkajšom priestore alebo na plášti objektu, budú inštalované zadné ochranné spínače pre indikáciu pokusu o strhnutie alebo narušenie. Výstupy budú zapojené do PZTS.

Jednotlivé detektory PZTS budú samostatne zapojené pomocou vyvážených poplachových slučiek na ústredňu PZTS alebo koncentrátory v súlade s požiadavkami ČSN EN 50131-1 ed.2 podľa príslušného stupňa zabezpečenia. Koncentrátory budú s ústredňou PZTS komunikovať po dátovej zbernici. Prepojenie jednotlivých prvkov PZTS s ústredňou a koncentrátormi bude vykonané metalickými káblami.

Prvky systému PZTS budú umiestnené nasledovne:

- priestorové detektory - na stene vo výške 220 až 240 cm od podlahy,
- detektory rozbitia skla - na stene alebo strope, minimálne 150 cm nad podlahou,
- magnetické kontakty - na rámoch dverí okien, dverí a brán z vnútornej strany stráženého priestoru,
- ovládacie prvky (snímače kariet, klávesnica) - na stene vo výške cca 150cm nad podlahou.

Pred priestorovými detektory nesmie byť umiestnený nábytok, police, kvety a obdobné predmety, ktoré by zhoršovali ich detekciu. Po inštalácii pohybových detektorov bude prekontrolovaný ich dosah a účinnosť. Priestorové detektory budú inštalované s ohľadom na zdroje tepla, ventilátory a klimatizáciu.

Ústredňa PZTS bude vybavená modulmi pre pripojenie k dátovej sieti LAN pre diaľkovú signalizáciu a ovládanie, vrátane možnosti správy užívateľov a konfigurácie ústredne. Prostredníctvom dátovej siete LAN bude možné prenášať dáta PZTS do grafického dohľadového softvéru v DPPC spoločnosti.

Programovanie a nastavenie systémových parametrov PZTS odporúčam z bezpečnostných dôvodov umožniť iba lokálne.

**Výber konkrétnych prvkov PZTS**

Kapitola obsahuje popis technických parametrov vybraných prvkov PZTS, ktoré budú nasadené v modelovom projekte.

- **Ústredňa PZTS - GALAXY GD-520**

Tabuľka 11: Technické parametre pre ústredňu PZTS (vlastné spracovanie)

| | |
|---|---|
| **Napájanie** | 16,5V, transformátor je súčasť balenia |
| **Počet zón na ústredni** | 16 |
| **Max. počet drôtových zón** | 520 |
| **Max. počet bezdrôtových zón** | 192 |
| **Počet blokov (subsystémov)** | 32 |

| | |
|---|---|
| **Automatické zapnutie/vypnutie** | Áno / Nie |
| **Spôsoby zapnutia** | kódom, bezdrôtovým ovládačom, SW, prístupovou kartou |
| **Vstavaný telefónny komunikátor** | áno |
| **Podpora IP komunikátoru (LAN, GPRS)** | áno |
| **Prístupová nadstavba** | áno |
| **Komunikačná frekvencia** | 868 MHz |
| **Bezdrôtová nadstavba** | áno |
| **Typy klávesníc** | LCD, LCD s čítačkou kariet, dotyková |
| **Počet klávesníc v systéme** | 32 |
| **Počet užívateľských kódov** | 1000 |
| **Počet bezdrôtových ovládačov** | 100 |
| **Pamäť udalostí** | 1500 |
| **Max. dĺžka zbernice** | 1000 m |
| **Max. prúdový odber z výstupov** | 1000 mA |
| **Prevedenie** | plošný spoj s krytom |

- **Komunikačný modul pre integráciu ústrední Galaxy, GXYSMART**

Tabuľka 12: Technické parametre pre komunikačný modul pre integráciu ústrední (vlastné spracovanie)

| | |
|---|---|
| **Typ modulu** | integračný modul |
| **Prevedenie** | oceľová skrinka |
| **Kompatibilita** | Galaxy GD, G3 |
| **Pripojenie** | linka 1 RS-485 |
| **Indikácia komunikácie s ústredňou** | áno, LED dióda |
| **Typ rozhraní** | RS-232 alebo TCP / IP |
| **Komunikačná rýchlosť** | 115 200Bd alebo 10 / 100Mbit |
| **Sabotážny kontakt** | áno |

- **Systémový GSM modul pre posielanie SMS - GXYSMART GSM**

Tabuľka 13: Technické parametre pre systémový GSM(vlastné spracovanie)

| | |
|---|---|
| **Kompatibilita** | Galaxy GD, G3 |
| **Počet SIM kariet** | 1 |
| **Počet tel. čísiel pre volanie** | 8 |
| **Počet tel. čísel SMS** | 8 |
| **Počet vstupov a výstupov** | 4 + 1 |
| **Typ výstupu** | 1 reléový, 2 typu otvorený kolektor |
| **Sabotážny kontakt** | mechanický mikro spínač |
| **Prevedenie** | v oceľovom kryte s GSM anténou |

| | |
|---|---|
| **Špeciálne funkcie** | pripojenie na RS-485 |
| **Napájacie napätie** | 11 - 13,8 V |
| **Spotreba - vysielanie** | 0,5 A |
| **Pracovná teplota** | 0 až 40 ° C |
| **Trieda prostredia** | vnútorné |
| **Rozmery - výška** | 240 mm |
| **Rozmery - šírka** | 240 mm |
| **Rozmery - hĺbka** | 65 mm |
| **Farba** | svetlo šedá |

- **Plastový magnetický kontakt MAS303**

Tabuľka 14: Technické parametre pre pastový magnetický kontakt MAS303 (vlastné spracovanie)

| | |
|---|---|
| **Montáž** | povrchová |
| **Upevnenie** | skrutka |
| **Max. pracovná vzdialenosť** | 20 mm |
| **Farba** | biela |
| **Teplota prevádzkové** | -40 až +70 °C |
| **Vstavané EOL odpory** | nie |
| **Počet vodičov** | 4 |
| **Poplachový výstup** | 1 |
| **Sabotážny kontakt** | áno |
| **Dĺžka prívodného kábla** | 300 cm |
| **Bezpečnostná trieda** | 3 |
| **Certifikát NBÚ** | áno |
| **Šírka** | 13 mm |
| **Výška** | 54 mm |
| **Hĺbka** | 13 mm |
| **Hmotnosť** | 0,1 kg |

- **Magnetický kontakt na brány, vyvážený, polarizovaný - DC115**

Tabuľka 15: Technické parametre pre Magnetický kontakt na brány DC115 (vlastné spracovanie)

| | |
|---|---|
| **Pracovná medzera** | 9 mm (min.); 62 mm (max.) |
| **Pripojenie (pancierovaný kábel)** | 5 vodičov; 2 m |
| **Typ kontaktu** | CO |
| **Šírka** | 76,2 mm |
| **Výška** | 12,7 mm |
| **Hĺbka** | 25,4 mm |
| **Kryt** | Anodizovaný hliník |

- **Duálny detektor pohybu - N033440.01**

Tabuľka 16: Technické parametre pre duálny detektor pohybu (vlastné spracovanie)

| | |
|---|---|
| **Typ** | PIR + MW |
| **Dosah PIR vejár - dĺžka** | 15 m |
| **Dosah MW - dĺžka** | 15 m |
| **Odporúčaná montážna výška** | 2,5 m |
| **Odber - nominálne** | 6,6 mA |
| **Odber - max.** | 11 mA |
| **Pamäť poplachu** | áno |
| **Antimasking** | áno |
| **Poplachový výstup** | NC, 15 V / 100 mA |
| **Sabotážny výstup** | NC, 15 V / 100 mA |
| **Citlivosť** | normálny / vysoká |
| **Indikácia poplachu** | LED dióda |
| **Pracovná teplota** | -10 až 55 ° C |
| **Rozmery - výška** | 158 mm |
| **Rozmery - šírka** | 64 mm |
| **Rozmery - hĺbka** | 48 mm |
| **Stupeň zabezpečení** | 3 |

- **TCP/IP (Xport) prvok do komunikačného modulu - GXYSMART**

Tabuľka 17: Technické parametre pre TCP/IP prvok do komunikačného modulu (vlastné spracovanie)

| | |
|---|---|
| **Typ** | voliteľný plug-in modul |
| **Ethernet** | 10 / 100Base-T |

- **Akustický detektor rozbitia skla s AM - AD800-AM**

Tabuľka 18: Technické parametre pre akustický detektor rozbitia skla (vlastné spracovanie)

| | |
|---|---|
| **Dosah** | 1m až max. 9m / 165° |
| **Poplachový výstup** | NC, 50 V / 50 mA |
| **Sabotážny kontakt** | NC, 50 V / 50 mA |
| **Napájacie napätie** | 7 - 30 V |
| **Špeciálne funkcie** | IR a akustický antimasking |
| **Odber - nominálne** | 12 mA |
| **Typy skiel** | tabuľové & kalené jednosklo, dvojsklo a trojsklo; tabuľové dvojsklo s ochranou |

| | |
|---|---|
| | fóliou; jednoduché lepené, s viacerými sklenenými tabuľami s vnútornou fóliou |
| **Minimálny rozmer skla** | 40 x 40 cm |
| **Nastavenie citlivosti** | áno, 3 úrovne podľa typu skla |
| **Pamäť poplachu** | áno |
| **Doporučený tester** | ADT700 |
| **Farba** | biela |
| **Trieda prostredia** | vnútorné |
| **Pracovná teplota** | 5 až 40 ° C |
| **Relatívna vlhkosť** | 0 - 93 % |
| **Rozmery - výška** | 110 mm |
| **Rozmery - šírka** | 69 mm |
| **Rozmery - hĺbka** | 39 mm |
| **Stupeň zabezpečenia** | 3 |
| **Antimasking** | áno |

- **Riadiaca jednotka pre pripojenie čítačiek na zbernicu Galaxy - MAXM2000**

Tabuľka 19: Technické parametre pre riadiacu jednotku pre pripojenie čítačiek (vlastné spracovanie)

| | |
|---|---|
| **Prevedenie** | kovový kryt |
| **Odber - pokojový** | 35 mA |
| **Odber - max.** | 55 mA |
| **Kompatibilita** | ústredne Galaxy GD, |
| **Indikácia komunikácie s ústredňou** | áno, LED dióda |
| **Počet pripojiteľných čítačiek** | 2 |
| **Výstup pre napájanie čítačiek** | 12 V, max. 200 mA |
| **Podporované formáty** | Wiegand 26, 27, 32, 34 a 40 bitov |
| **Kontrola opakovanej neplatnej karty** | áno (voliteľné prepojkou) |
| **Podporované čítačky Motorola Indala** | ASR603, ASR605, ARK501 atď. |
| **Podporované čítačky HID** | PROXPOINT PLUS, MINIPROX atď. |
| **Podporované čítačky MIFARE** | MIFARE 13.56MHz 32bit, MIFARE čítačka 34bit |
| **Podporované čítačky EM** | EM čítačka 32 bit, EM RDR 26 bit |
| **Podporované čítačky Dallas** | D-TANGO |
| **Biometrické čítačky a iné čítačky** | na vyžiadanie |
| **Relé pre ovládanie zámkov** | 2x zdvojené relé (max. zaťaženie 2 A) |
| **Dverný kontakt** | 2x (NC) |
| **Odchodové tlačidlo** | 2 x (NO) |
| **Armovacie tlačidlo** | 2 x (NO) |
| **Sabotážny kontakt** | áno |
| **Farba** | šedá |

- **Bezkontaktná čítačka kariet - RSW.04**

Tabuľka 20: Technické parametre pre bezkontaktnú čítačku kariet (vlastné spracovanie)

| | |
|---|---|
| **Typ čítačky** | bezkontaktné |
| **Napájacie napätie** | 9 - 15 V |
| **Odber** | 100 mA |
| **LED dióda** | 2-farebná |
| **Bzučiak** | áno |
| **Farba krytu** | čierna |
| **Krytie** | IP 65 |
| **Pracovná teplota** | -25 - 60 °C |
| **Rozmery - výška** | 117 mm |
| **Rozmery - šírka** | 44 mm |
| **Rozmery - hĺbka** | 20 mm |
| **Kompatibilná karta** | Mifare 1K Karta |
| **Kompatibilný prívesok** | Mifare 1K Tag |
| **Kompatibilný nalep. TAG** | Mifare 1K Tag |
| **Špeciálne funkcie** | Načítanie ID čísla z NFC smartfónu (Android) - vyžaduje kompatibilitu aplikácii |
| **Použitie v exteriéri** | áno |
| **Technológia** | Mifare; DESFire; Mifare Plus; NFC |
| **Pracovná frekvencia** | 13,56 MHz |
| **Výstupný formát** | Wiegand |
| **Max. čítací dosah** | 5 cm |

### 3.5.2 Dohľadový videosystém

Inštalovaný videosystém bude snímať priestor hlavného vjazdu do areálu, celý perimeter areálu a vybrané vnútornej časti objektov v areáli. Prehľad o aktuálnej situácii umožňuje v prípade potreby prijať primerané opatrenia na zabezpečenie ochrany majetku.

Obrazový záznam zo všetkých kamier bude ukladaný na lokálne záznamové zariadenie NVR. ktoré bude umiestnené v dátovom rozvádzači STO vo VF miestnosti 3. NP.

Systém bude napojený na DPPC po existujúcej privátnej sieti LAN. Prepojenie umožňuje spätnú kontrolu napríklad pri udalosti, signalizovanej PZTS, alebo v prípade mimoriadnych prevádzkových stavov.

Podľa požiadavky spoločnosti nesmie byť vyvedená IP sieť a IP komunikácia mimo perimetra budovy. Celý VSS je preto navrhnutý na platforme "analógových" HD kamier. Sú to systémy, distribuované na trhu pod označením napr. HDTV, Turbo HD a podobne.

Ovládanie otočných kamier bude zabezpečené prostredníctvom ovládacej klávesnica s joystickom. Signalizácia stavov VSS bude vyvedená diaľkovo na DPPC prostredníctvom dátového prepojenia LAN.

Signalizované budú minimálne tieto stavy:

- porucha kamery (výpadok signálu),
- zakrytie kamery,
- zmena záberu (zmena sledovanej scény alebo nadmerné zníženia kvality obrazu).

V prípade udalosti v PZTS dôjde k automatickému zopnutiu vybranej kamery, alebo skupiny kamier na monitor dohľadového SW. Operátor bude mať ďalej možnosť spustiť si prehrávanie záznamu z času pred vznikom udalosti.

Pre VSS sú navrhnuté nasledujúce parametre záznamu:

- doba záznamu 30 dní,
- záznam všetkých kamier v plnom (maximálnom) rozlíšení,
- snímacia rýchlosť 15 snímok/sek,
- kompresný algoritmus H.264.

Pri maximálnej kvalite obrazu vychádza dátový tok na všetky kamery 28,2Mbps a potrebný záznamový priestor pre 30 dní záznamu činí cca 8,46 TB.

Skutočný dátový tok z kamier môže byť nižší, (priemerne cca 1-2 Mbps), ktorý závisí aj od svetelných podmienok snímanej scény (úroveň šumu), intenzity pohybu v scéne a použitom kompresnom algoritme.

### Ochrana osobných údajov

Prevádzkovanie kamerového systému je považované za spracovanie osobných údajov, pokiaľ je okrem kamerového sledovania vykonávaný záznam zhotovovaných záberov alebo sú v zariadení uchovávané informácie, a zároveň účelom zhotovovaných záznamov, prípadne vybraných informácií, je ich využitie na identifikáciu fyzických osôb v súvislosti s určitým konaním. (14)

Údaje uložené v záznamovom zariadení, obrazové alebo zvukové, sú osobnými údajmi za predpokladu, že na základe týchto údajov možno priamo alebo nepriamo identifikovať konkrétnu fyzickú osobu. (14)

Na základe vyššie uvedených stanovísk Úradu pre ochranu osobných údajov sa musia pri návrhu kamerového systému so záznamom rešpektovať požiadavky zákona č. 101/2000 Sb. O ochrane osobných údajov a o zmene niektorých zákonov v znení neskorších predpisov. Prevádzkovateľ kamerového systému so záznamom, je teda považovaný podľa zákona č. 101/2000 Sb. za správcu osobných údajov. (14)

Zásady a usmernenia pre registráciu a prevádzku VSS nie sú predmetom tejto práce a preto sa nimi nebude ďalej zaoberať.

### Výber konkrétnych prvkov VSS

Kapitola obsahuje popis technických parametrov vybraných prvkov VSS, ktoré budú nasadené v modelovom projekte.

- **LED dotykový monitor - ASUS VT168H**

Tabuľka 21: Technické parametre pre LED dotykový monitor (vlastné spracovanie)

| | |
|---|---|
| **Uhlopriečka displeja** | 15,6" |
| **Rozlíšenie** | 1366 × 768 px (1366 × 768 px px) |
| **Pomer strán** | 16:9 |
| **Technológia** | LCD LED |

| | |
|---|---|
| **Typ obrazovky** | Rovná |
| **Jas** | 200 cd/m2 |
| **Povrch displeja** | Lesklý |
| **Grafické vstupy** | HDMI 1.4 a starší, D-SUB (VGA) |
| **Výbava** | Dotyková obrazovka, VESA kompatibilný |
| **Funkcie** | Filter modrého svetla |
| **Typická spotreba** | 7 W |
| **Stand-by spotreba (pohotovostná)** | 0,5 W |
| **Farba** | Čierna |
| **Šírka** | 37,78 cm |
| **Výška** | 28,07 cm |
| **Hĺbka** | 18,94 cm |
| **Hĺbka bez podstavca** | 44 mm |

- **Záznamové zariadenie - DS 7216HUHI-F2/N**

Tabuľka 22: Technické parametre pre záznamové zariadenie (vlastné spracovanie)

| | |
|---|---|
| **Video kompresia** | H.264 + / H.264 |
| **HD-TVI vstup** | 1080p / 25Hz, 1080p / 30Hz, 720p / 25Hz, 720p / 30Hz, 720P / 50Hz, 720p / 60Hz, 3Mpx |
| **HD vstup** | 720p / 25Hz, 720p / 30Hz |
| **IP video vstup** | 2-ch až 4 Mpx rozlíšenie |
| **Audio kompresia** | G.711 |
| **HDMI/VGA výstup** | VGA: 1-ch, 1920 x 1080/60 Hz, 1280 x 1024/60 Hz, 1280 x 720/60 Hz, 1024 x 768 / 60Hz, HDMI: 1-ch, 4K (3840 x 2160) / 30 Hz, 2K (2560 x 1440 ) / 60Hz, 1920 x 1080/60 Hz, 1280 x 1024/60 Hz, 1280 x 720/60 Hz, 1024 x 768 / 60H |
| **Rozlíšenie kódovanie** | 3MP / 1080p / 720p / WD1 / 4CIF / VGA |
| **Snímkovanie** | Hlavný prúd: 3Mpx @ 15fps; 1080p / 720p / VGA |
| **Prenosová rýchlosť video** | 32 Kbps - 10 Mbps |
| **Audio výstup** | 1-ch, RCA (lineárne, 1 KΩ) |
| **Prenosová rýchlosť audio** | 64 Kbps |
| **2x Stream** | podporované |
| **Typ streamu** | Video, video a zvuk |
| **Synchrónne prehrávanie** | 16-ch |
| **vzdialené pripojenie** | 128 |
| **Protokoly** | TCP / IP, PPPoE, DHCP, Hik Cloud P2P, DNS, DDNS, NTP, SADP, NFS, iSCSI, |

| | |
|---|---|
| | UPnP, HTTPS, ONVIF |
| **SATA** | 2 SATA |
| **Kapacita** | až 6TB pre každý disk |
| **Sieťové rozhranie** | 1x RJ45 10M / 100M / 1000M samoadaptívny Ethernet |
| **USB rozhranie** | predný panel: 1 × USB 2.0, zadný panel: 1 × USB 3.0 |
| **Sériové rozhranie** | RS485 |
| **Napájanie** | 12V DC |
| **Prevádzkové teploty** | -10 ℃ - +55 ℃ |
| **Prevádzková vlhkosť** | 10% - 90% |
| **Šírka** | 38 cm |
| **Výška** | 32 cm |
| **Hĺbka** | 48 cm |
| **Váha** | 2,2 kg |

- **Pevný disk - Seagate SkyHawk 6TB**

Tabuľka 23: Technické parametre pre pevný disk (vlastné spracovanie)

| | |
|---|---|
| **Typ úložiska** | HDD |
| **Formát** | 3,5" |
| **Kapacita disku** | 6 TB |
| **Šírka** | 101,6 mm (10,16 cm) |
| **Výška** | 26,1 mm (2,61 cm) |
| **Hĺbka** | 147 mm (14,7 cm) |
| **Rozhranie interné** | SATA III |
| **Vyrovnávacia pamäť** | 64 MB |
| **Rýchlosť otáčok HDD** | 7 200 otáčok za minútu |
| **Funkcie** | RAID, Advanced Format |

- **Vonkajšia kamera - DS-2CE16D9T-AIRAZH**

Tabuľka 24: Technické parametre pre vonkajšiu kameru (vlastné spracovanie)

| | |
|---|---|
| **Prevedenie kamery HD-TVI** | Bullet kamery s IR |
| **Počet megapixelov** | 2 megapixely |
| **Dĺžka IR prísvitu** | 110 metrov |
| **Typ objektívu** | motorický |
| **Napájanie** | DC12V / AC24V |
| **Horizontálny uhol (maximálny)** | 85° |
| **Režim Deň/Noc** | IR-cut |
| **Spotreba** | 10-20 W |

| | |
|---|---|
| **Technológia** | HD-TVI |
| **Prevedenie** | vonkajšie |
| **Objektív** | 5 - 50 mm |
| **WDR** | 120dB |
| **Maximálne rozlíšenie** | 1920 x 1080, 25 fps |
| **Veľkosť zoomu** | 10x zoom |
| **Citlivosť** | štandardné |
| **Ovládacie rozhranie** | koaxiál / RS485 |
| **Stupeň krytí IP** | IP66 |
| **Prevádzková teplota** | -30° až +60° C |

- **Vnútorná kamera - DS-2CE56D7T-AITZ**

Tabuľka 25: Technické parametre pre vnútornú kameru (vlastné spracovanie)

| | |
|---|---|
| **Prevedenie** | vnútorné |
| **Počet megapixelov** | 2 Mpix |
| **IR prísvit** | 30 metrov |
| **Typ objektívu** | motorický |
| **Stupeň krytí IP** | IP 65 |
| **Citlivosť** | štandardná |
| **Režim deň/noc** | IR-cut |
| **WDR** | 120 dB |
| **Max. uhol** | 120° |
| **Napájanie** | DC 12 V / AC 24 V |
| **Spotreba** | 5 - 10 W |
| **Prevádzková teplota** | -40°C až 60°C |

- **Otočná PTZ kamera DS-2DE3204W-DE**

Tabuľka 26: Technické parametre pre otočnú PTZ kameru (vlastné spracovanie)

| | |
|---|---|
| **Podporované umiestnenie** | Vnútorné, Vonkajšie |
| **PTZ ovládanie (Pan-Tilt-Zoom)** | Áno |
| **Široký dynamický rozsah** | Áno |
| **Režim deň/noc** | Áno |
| **Alarm vstup/výstup** | Áno |
| **Infračervený (IR)** | Áno |
| **Typ** | Dome |
| **Spôsob montáže** | Strop, stena |
| **Kód medzinárodnej ochrany (IP)** | IP66 |
| **Maximálne rozlíšenie** | 1920 x 1080 |
| **Kompresné formáty videa** | H.264,M-JPEG |

| | |
|---|---|
| **Uhol zorného poľa** | 105° |
| **Uhol náklonu** | 0 - 90° |
| **Rýchlosť nakláňania** | 50° za sek. |
| **Rozsah otáčania** | 0 - 350 ° |
| **Rýchlosť otáčania** | 60° za sek. |
| **Možnosti zoomu** | Áno |
| **Optický zoom** | 4 x |
| **Digitálny zoom** | 16 x |
| **Ohnisková vzdialenosť** | 2.8 - 12 mm |
| **Nočné videnie** | Áno |
| **Výška** | 107.2 mm |
| **Priemer** | 140.7 mm |
| **Hmotnosť** | 950 gramov |
| **DC výstupné napätie** | 12 V |
| **Spotreba energie (max)** | 8 W |
| **Prevádzkový rozsah teplôt (T-T)** | od -30°C do +65°C |

**Spôsob a umiestnenie prvkov VSS**

Pevné HD kamery budú umiestnené na existujúcich konštrukciách budov a na nových kamerových stožiaroch a budú vybavené externým IR prisvietením s dosahom podľa projektovanej vzdialenosti sledovanej scény. IR prísvit bude umiestnený vo vzdialenosti 0,75-1 m pod kamerou pre elimináciu falošných poplachov prilákanými hmyzom. Kamery budú umiestnené vo výške cca 4 m.

Pre identifikáciu musí byť zaistené sledovanie a záznam scény v rozlíšení najmenej 250 pixelov na meter. V prípade kamery s FullHD rozlíšením to znamená maximálnu šírku sledovanej scény 8m.

U 360° kamery s rozlíšením 5 Megapixelov to zodpovedá sledovaniu scény vo vzdialenosti do cca 1,65 m (pre výpočet som použil kameru s rozlíšením 2592x1944 pixelov)

### 3.5.3 Zónovanie, režim vstupu do zón

Riadenie prístupu osôb do areálu aj do budov bude súčasťou systému PZTS. Ústredňa PZTS bude vyhodnocovať oprávnenia prístupu držiteľov ID kariet. V pamäti ústredne PZTS bude uložená história priechodov.

Vybrané dvere a vjazdová brána a bránka budú ovládané bezkontaktnou kartou, ktorá bude prikladaná k snímaču, umiestnenému v blízkosti vybraného miesta. Prístupový modul snímača vyhodnotí oprávnenia prístupu a odblokuje elektromechanický zámok alebo povolí otvorenie brány.

Pre zaistenie spoľahlivého prenosu dát zo snímačov kariet budú ich riadiace jednotky umiestnené neďaleko vjazdu do samostatného vonkajšieho rozvádzača spoločne s koncentrátorom pre pripojenie magnetických kontaktov a napájacím zdrojom. Riadiace jednotky a koncentrátor komunikujú s ústredňou pomocou rozhrania RS485.

### 3.5.4 Ekonomické zhodnotenie

V tejto podkapitole návrhovej časti predstavujem súhrn nákladov pre EZS celého navrhovaného projektu pre modelový objekt. Nasledujúca tabuľka č. 27 obsahuje súhrnné čiastky v českých korunách a tak stanovuje celkový rozpočet potrebný pre realizáciu modelového objektu. Dielčie čiastky a detailnejší popis rozpočtu je znázornený v prílohe číslo 5.

Tabuľka 27: Výsledný rozpočet. (vlastné spracovanie)

| Názov | Cena celkom bez DPH | DPH 21% | Cena celkom s DPH |
|---|---|---|---|
| **Poplašné zabezpečovacie a tiesňové systémy** | 478 981,00 Kč | 100 586,01 Kč | 579 567,01 Kč |
| **Dohľadové videosystémy** | 161 308,00 Kč | 33 874,68 Kč | 195 182,68 Kč |
| **Materiál** | 642 280,00 Kč | 134 878,80 Kč | 777 158,80 Kč |
| **Inštalácia** | 705 412,95 Kč | 148 136,72 Kč | 853 549,67 Kč |
| **Spolu** | 1 987 981,95 Kč | 417 476,21 Kč | **2 405 458,16 Kč** |

Stanovený rozpočet počíta len s nákladmi na konkrétne prvky zabezpečovacích systémov, materiál potrebný na ich inštaláciu a cenu práce za inštaláciu.

## 3.6 Zhodnotenie a prínos práce

Hlavným a zásadným prínosom tejto práce a v nej obsiahnutom je návrh elektronického zabezpečovacieho systému pre energetickú spoločnosť vrátane systému na evidenciu

kontroly vstupu do jednotlivých objektov spoločnosti. Dielčím prínosom je zjednotenie úrovne fyzického zabezpečenia vo všetkých objektoch kritickej infraštruktúry.

Tento systém bude postupne zavádzaný najmä z dôvodu:

- splnenia požiadaviek noriem a interným predpisov spoločnosti,
- splnenia platnej legislatívy pre ochranu prvkov kritickej infraštruktúry,
- zvýšenia ochrany majetku a osôb spoločnosti,
- prípravy reálneho stavu zabezpečenia pre prípadnú certifikáciu rady ISO 27 000.

Zavedenie navrhovaného EZS má pre spoločnosť aj priamy ekonomický prínos. Spracovanie všeobecných podmienok pre výber EZS bude slúžiť ako podklad pre výberové konanie dodávateľa daných systémov. V praxi si zhotovitelia všeobecných podmienok a návrhovej časti účtujú 2% z plánovaného rozpočtu celkovej investície projektu. Nakoľko celková plánovaná cena projektu s DPH predstavuje čiastku cca 2,4 mil. Kč, prínosom je ušetrenie nákladov v hodnote cca 48 tis. Kč na jeden konkrétny objekt. Spoločnosť bude realizovať implementáciu EZS v približne 120 objektoch KI a tým pádom celkové ušetrené náklady činia približne 5 773 000 Kč. Do budúcnosti je však nutné počítať s prevádzkovými nákladmi systému vyššími, než sú existujúce. Okrem iného bude potrebné preškoliť pracovníkov strážnej služby na používanie nového systému.

Ďalším prínosom pre spoločnosť je zníženie niektorých rizík, ktoré hrozia vyplývajú z vypracovanej analýzy rizík a systém pre evidenciu kontroly vstupu je navrhnutý tak, aby bol ďalej rozšíriteľný na ďalšie možné účely. Celkom iste ho bude možné prepojiť s dochádzkovým systémom. Bezkontaktné karty prístupového systému by mohli byť v budúcnosti používané napríklad pre prístup do služobných vozidiel.

# ZÁVER

Diplomová práca sa zaoberala návrhom elektronických zabezpečovacích systémov ako časť fyzického zabezpečenia prvkov kritickej infraštruktúry pre energetickú spoločnosť. Zavedením elektronických zabezpečovacích systémov možno sledovať navýšenie fyzickej bezpečnosti a celkové zvýšenie ochrany majetku a osôb spoločnosti pri súčasnom naplnení legislatívnych podmienok a požiadaviek interných predpisov spoločnosti.

Všeobecné teoretické pojmy sú opísané v úvodnej časti "Teoretické východiská práce“

Časť „Analýza súčasného stavu“ sa zamerala na charakteristiku sektoru energetiky, popis legislatívnych a regulačných obmedzení v odvetví, predstavenie spoločnosti a súčasný stav fyzickej bezpečnosti v stanovenom rozsahu. Súčasťou bola analýza spoločnosť externých a interných faktorov, za použitia špecifických metód. Výsledky týchto analýz boli spracované pomocou SWOT analýzy, ktorá popisuje silné, slabé stránky, hrozby a príležitosti plynúce z realizácie daného projektu. Na záver bola zhotovená analýza rizík, ktorá stručne popisuje možné riziká a stanovuje opatrenia, aby sa týmto rizikám predchádzalo.

Časť „Vlastné návrhy riešenia“ obsahuje súpis všeobecných technických požiadaviek na EZS tak, aby splňovali legislatívu a technické normy, ktorými sa musí spoločnosť riadiť. Ako hlavný zdroj požiadaviek bola využitá predbežná česká štátna norma 73 4450-1. Následne sa v nej navrhujú konkrétne parametre prvkov poplašných zabezpečovacích a tiesňových systémov a dohľadových videosystémov, ktoré budú slúžiť ako podklad pre výberové konanie na dodávateľa daných elektronických zabezpečovacích systémov Súčasťou návrhovej časti je aj ekonomické zhodnotenie s odhadom jednorazových nákladov na realizáciu projektu, ktorá vychádza z modelového objektu. V závere časti boli uvedené prínosy diplomovej práce pre energetickú spoločnosť pri zavádzaní EZS do objektov KI spoločnosti, na základe ktorých možno usúdiť, že vymedzené ciele diplomovej práce boli dosiahnuté.

# ZOZNAM POUŽITÝCH ZDROJOV

(1) JORDÁN, V. a V. ONDRÁK. *Infrastruktura komunikačních systémů II: Kritické aplikace*. Brno: CERM, 2015. ISBN 978-80-214-5240-4

(2) ČSN ISO/IEC 27000. *Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Přehled a slovník*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

(3) ČSN ISO/IEC 27001. *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

(4) DOUCEK P., V. NOVÁK a V. SVATÁ. *Řízení bezpečnosti informací, Praha: Professional Publishing*, 2008. ISBN 80-86898-38-5.

(5) ONDRÁK V., P. SEDLÁK a V. MAZÁLEK. *Problematika ISMS v manažerské informatice. Brno: CERM, Akademické nakladatelství*, 2013. ISBN 978-80-7204-872-4

(6) ČSN P 73 4450-1. *Fyzická ochrana prvku kritické infrastruktury. Část 1, Obecné požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

(7) ČSN EN 50131-1 ed. 2. *Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 1: Systémové požadavky*. Praha: Český normalizační institut, 2007.

(8) NÚKIB. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. 2011 [cit. 2018-03-27]. Dostupné z: http://www.govcert.cz

(9) ČSN EN 62676-1-1. *Dohledové videosystémy pro použití v bezpečnostních aplikacích*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

(10) ČSN EN 60839-11-1. *Poplachové a elektronické bezpečnostní systémy - Část 11-1: Elektronické systémy kontroly vstupu - Požadavky na systém a komponenty*. Praha: Český normalizační institut, 2014.

(11) BURIAN, D. K některým povinnostem, které pro správce přináší Obecné nařízení o ochraně osobních údajů (GDPR). *PRÁVNÍ PROSTOR* [online]. 2016 [cit. 2018-03-28]. ISSN 2336-4114. Dostupné z: http://www.pravniprostor.cz/clanky/ostatni-pravo/k-nekterym-povinnostem-ktere-pro-spravce-prinasi-gdpr

(12) Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) ze dne 23. července 2014

(13) Zákon č. 458/2000 Sb., o podmínkách podnikání a o výkonu státní správy v energetických odvětvích a o změně některých zákonů (energetický zákon) ze dne 28. listopadu 2000.

(14) Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů ze dne 4. dubna 2000.

(15) DURAČINSKÁ, Z. *Co přináší nová směrnice EU o informační bezpečnosti? IT Systems* [online]. 2016, [cit. 2018-03-25]. ISSN 1802-615X. Dostupné z: https://www.systemonline.cz/clanky/co-prinasi-nova-smernice-eu-o-informacni-bezpecnosti.htm

(16) ČSN ISO/IEC 27005. *Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

(17) ČSN ISO/IEC 27002. *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Soubor postupů pro opatření bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014

(18) ISO/IEC TR 27019:2013. *Information technology – Security techniques – Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry*. Geneva: International Organization for Standardization, 2013.

(19) Nařízení vlády č. 315/2014 Sb. o kritériích pro určení prvku kritické infrastruktury ze dne 8. prosince 2014.

(20) Zákon č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů (krizový zákon) ze dne 28. června 2000.

(21) Nařízení vlády č. 432/2010 Sb. kritériích pro určení prvku kritické infrastruktury ze dne 22. prosince 2010.

# ZOZNAM TABULIEK

# ZOZNAM OBRÁZKOV

# ZOZNAM SKRATIEK

ABI – Advanced building intelligence

AM – Antimasking

BOZP – Bezpečnosť a ochrana zdravia pri práci

CCTV - Closed-circuit television

CERT - Computer Emergency Response Team

CSIRT - Computer Security Incident Response Team

ČR - Česká republika

ČSN – Česká štátna norma

D – Dopad

DDNS – Dynamic DNS

DHCP - Dynamic host configuration protocol

DNS – Domain name server

DPCA – Plan, do, check, act

DPPC - Dohľadové a prijímacie poplachové centrum

DPPC - Dohľadové a poplachové prijímacie centrum

EKV - Elektronický systém kontroly vstupu

EN – Europian norm

EOL - End of line

EPS - Elektrická požiarna signalizácia

ES – Energetická spoločnosť

EÚ – Európska únia

EZS – Elektronické zabezpečovacie systémy

fps – Frame per second

FTP – File tranfer protocol

FTP - Foiled twisted pair

GD – Galaxy dimension

GDPR - General data protection regulation

GSM – Globálny systém pro mobilnú komunikáciu

H – Hodnota rizika

HD – High definition

HDMI – High-definition multimedia interface

HDTV - High definition television

HTTP - Hypertext transfer protocol

HTTPs – Hypertext transfer protocol secured

HW - Hardware

ICMP - Internet control message protocol

IEC - International Electrotechnical Commission

IPv6 – Internet protocol version 6

IR - Infrared radiation

IS – Informačný systém

ISO - International Organization for Standardization

IT – Informačné technológie

Kbps – Kilobits per second

KI – Kritická infraštruktúra

KII – Kritická komunikačná infraštruktúra

LAN – Local area network

LCD - Liquid crystal display

LED – Light emitting diode

Mbps – Megabits per second

MN - Malé napätie

MZP - Mechanické zábranné prostriedky

NBÚ – Národný bezpečnostný úrad

NCPRS – Národné centrum PRS

NIS - Network and information systems

NN – Nízke napätie

NTP – Network time protocol

NÚKIB - Národný úrad pre kybernetickú a informačnú bezpečnosť

NVR - Network video recorder

P – Pravdepodobnosť

PIN - Personal identification number

PPPoE - Point-to-point protocol over ethernet

PRS - Public regulated service

PTZ - Pan-tilt-zoom

PZTS - Poplašný zabezpečovací a tiesňový systém

RS – Rozvodná stanica

RSTP – Rapid spanning tree protocol

RTCP – RTP control protoco

RTP – Real-time transport protocol

SATA – Serial ATA

SKV - Systémy kontroly vstupu

SMS - Short Message Service

SMTP – Simple mail transfer protocol

STO - Systém technickej ochrany

SW - Software

SZ – Stupeň zabezpečenia

TB – Terabajt

TCP/IP - Transmission control protocol / internet protoco

UNV - Ultra-vysoké napätie

USB – Universal serial bus

UTP - Unshielded twisted pair

VGA - Video Graphics Array

VIS – Významné informačné systémy

VMS – Systém videomanažmentu (video management system)

VN – Vysoké napätie

VSS - Dohľadový videosystém (video surveillance system)

VVN – Veľmi vysoké napätie

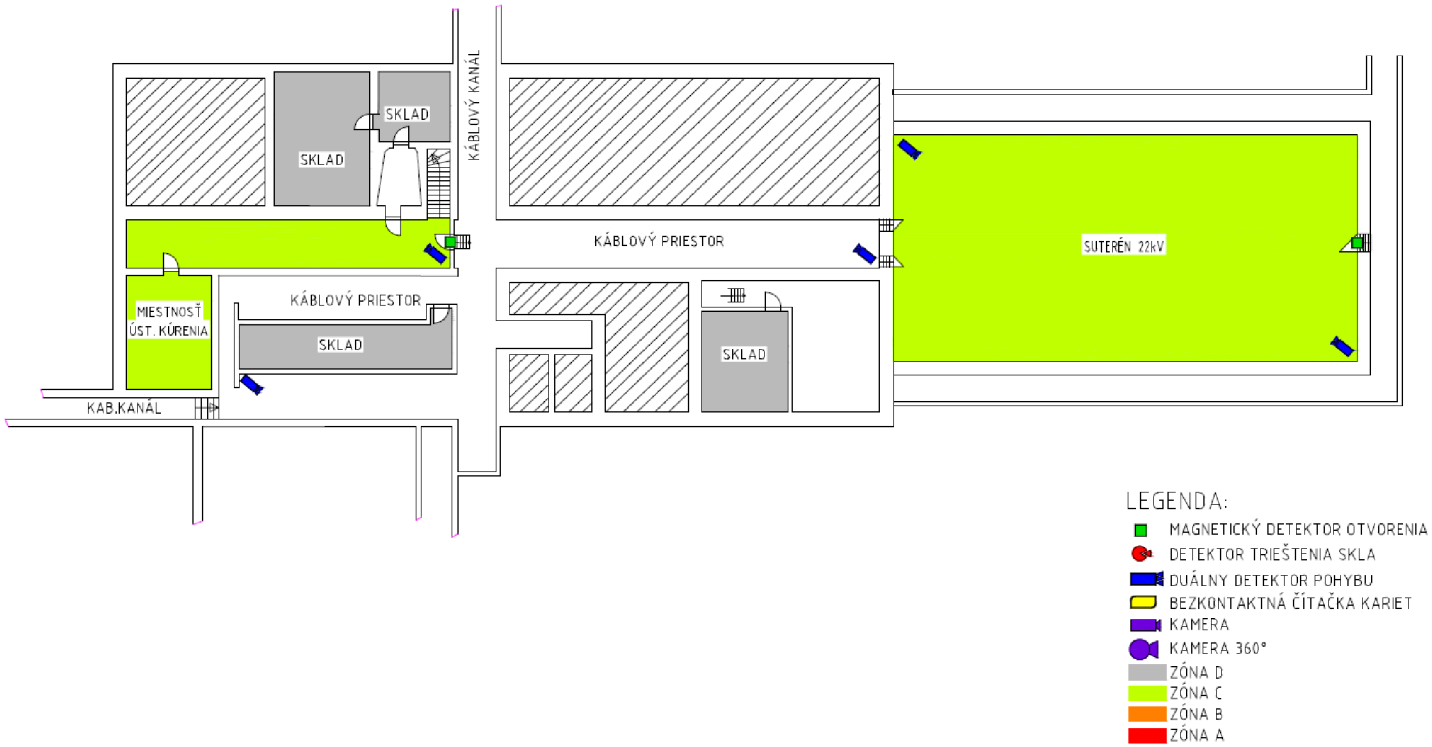
WDR - Wide dynamic range

ZVN - Zvlášť vysoké napätie

# ZOZNAM PRÍLOH

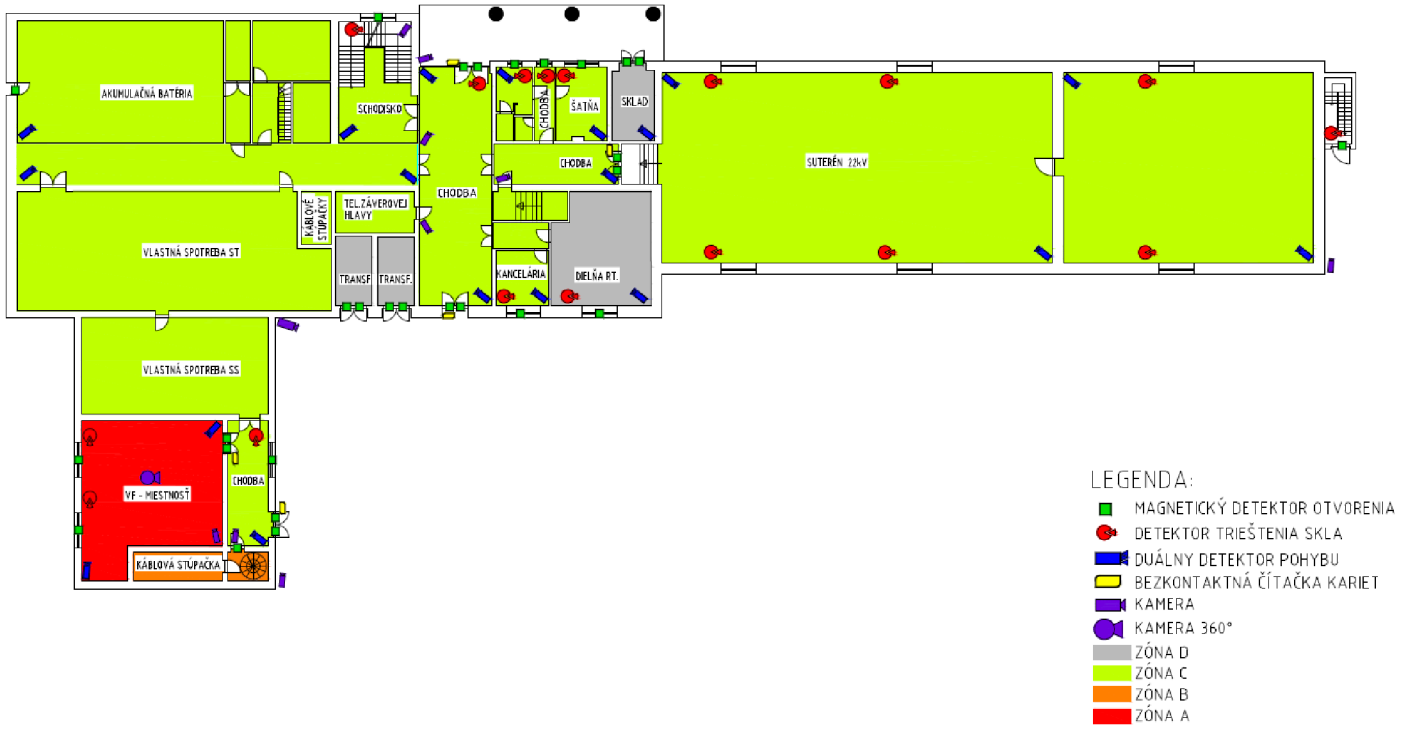
## Príloha 1: Pôdorys 1. podzemné podlažie

PÔDORYS 1 PP



## Príloha 2: Pôdorys 1. nadzemné podlažie

PÔDORYS 1 NP



## Príloha 3: Pôdorys 2. nadzemné podlažie

PÔDORYS 2 NP

## Príloha 4: Pôdorys 3. nadzemné podlažie

PÔDORYS 3 NP

**Príloha 5: Rozpočet bez DPH**

| Kód | Popis | MJ | Množstvo | Cena za MJ | Cena celkom bez DPH |
|---|---|---|---|---|---|
| **Poplašné zabezpečovacie a tiesňové systémy** | | | | | |
| **GALAXY GD-520** | Ústredňa PZTS | kus | 1 | 24 794,00 Kč | 24 794,00 Kč |
| **GXYSMART** | Komunikačný modul pre integráciu ústrední Galaxy | kus | 2 | 8 469,00 Kč | 16 938,00 Kč |
| **GXYSMART GSM** | Systémový GSM modul pre posielanie SMS | kus | 1 | 9 919,00 Kč | 9 919,00 Kč |
| **MAS303** | Plastový magnetický kontakt | kus | 43 | 298,00 Kč | 12 814,00 Kč |
| **DC115** | Magnetický kontakt na brány, vyvážený, polarizovaný | kus | 2 | 1 741,00 Kč | 3 482,00 Kč |
| **N033440.01** | Duálny detektor pohybu | kus | 56 | 3 523,00 Kč | 197 288,00 Kč |
| **GXYSMART TCPIP** | TCPIP (Xport) do komunikačného modulu | kus | 1 | 3 991,00 Kč | 3 991,00 Kč |
| **AD800-AM** | Akustický detektor rozbitia skla s AM | kus | 53 | 2 402,00 Kč | 127 306,00 Kč |
| **MAXM2000** | Riadiaca jednotka pre pripojenie čítačiek na zbernicu Galaxy | kus | 4 | 5 126,00 Kč | 20 504,00 Kč |
| **RSW.04** | Bezkontaktná čítačka kariet | kus | 13 | 4 765,00 Kč | 61 945,00 Kč |
| | Medzisúčet | | | | 478 981,00 Kč |
| **Dohľadové videosystémy** | | | | | |
| **ASUS VT168H** | LED dotykový monitor | kus | 1 | 3 298,00 Kč | 3 298,00 Kč |
| **DS 7216HUHI-F2/N** | Záznamové zariadenie | kus | 1 | 15 440,00 Kč | 15 440,00 Kč |
| **Seagate SkyHawk 6TB** | Pevný disk | kus | 2 | 3 776,00 Kč | 7 552,00 Kč |
| **DS-2CE16D9T-AIRAZH** | Vonkajšia kamera | kus | 4 | 6 006,00 Kč | 24 024,00 Kč |
| **DS-2CE56D7T-AITZ** | Vnútorná kamera | kus | 10 | 3 300,00 Kč | 33 000,00 Kč |
| **DS-2DE3204W-DE** | Otočná PTZ kamera | kus | 7 | 11 142,00 Kč | 77 994,00 Kč |
| | Medzisúčet | | | | 161 308,00 Kč |
| **Ostatné náklady** | | | | | |
| **Ostatný Materiál** | | | | | 642 280,00 Kč |
| **Inštalačné práce** | | | | | 705 412,95 Kč |
| **Náklady bez DPH celkom** | | | | | **1 987 981,95 Kč** |