

Návrh zabezpečení objektu vysoké školy

Bc. Vlastimil Krejčí

Diplomová práce
2018



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2017/2018

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Vlastimil Krejčí**
Osobní číslo: **A16236**
Studijní program: **N3902 Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**
Forma studia: **kombinovaná**

Téma práce: **Návrh zabezpečení objektu vysoké školy**
Téma anglicky: **Designing Security Measures for University Buildings**

Zásady pro vypracování:

1. Pojednejte o požadavcích technických a právních předpisů na zabezpečení objektů vysokých škol.
2. Analyzujte charakteristické vlastnosti objektů vysokých škol z hlediska možnosti jejich zabezpečení.
3. Popište moderní technologie zabezpečení aplikovatelné v objektech vysokých škol.
4. Na modelovém příkladu proveďte bezpečnostní posouzení objektu.
5. Zpracujte návrh zabezpečení modelového objektu.



Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. VALOUCH, Jan. Projektování bezpečnostních systémů. [skriptum]. Zlín: UTB, 2012. ISBN 978-80-7454-230-5. 152 s.
2. VALOUCH, Jan. Projektování integrovaných systémů. [skriptum]. Zlín: UTB, 2015. ISBN 978-80-7454-557-3 169 s.
3. ČSN CLC/TS 50131-7. Poplachové systémy- Poplachové zabezpečovací a tísňové systémy – Část 7: Pokyny pro aplikace. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011. 44 s. Třídící znak 334591.
4. UHLÁŘ, J. Technická ochrana objektů: II. díl. Elektrické zabezpečovací systémy. 1. vyd. Praha: Policejní akademie České republiky, 2005. 230 s. ISBN 80-7251-189-0.
5. KŘEČEK Stanislav. Příručka zabezpečovací techniky. Vydání 3. Blatná: Cricetus, 2006. 315 s. ISBN 80-902938-2-4.
6. LOVEČEK, T., NAGY, P. Bezpečnostné systémy: kamerové bezpečnostné systémy. Žilina: Žilinská univerzita v Žilíně, 2008. 272 s. ISBN 978-80-8070-893-1.

Vedoucí diplomové práce:

Ing. Jan Valouch, Ph.D.

Ústav bezpečnostního inženýrství

Datum zadání diplomové práce:

8. prosince 2017

Termín odevzdání diplomové práce:

28. května 2018

Ve Zlíně dne 8. prosince 2017



doc. Mgr. Milan Adámek, Ph.D.
děkan



doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že


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

Prohlašuji,

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

Ve Zlíně, dne

24.5.2018


.....
podpis diplomanta

ABSTRAKT

Diplomová práce řeší problematiku zabezpečení objektů vysokých škol, charakterizuje specifické vlastnosti vybraných prostor z hlediska potřeb jejich zabezpečení včetně analýzy požadavků relevantních právních a technických předpisů v dané oblasti. Záměrem práce je rovněž zpracování popisu moderních technologií pro zabezpečení specifických prostor vysokých škol. V diplomové práci je zpracováno srovnání vytypovaných prostor v dotčených objektech z hlediska potřeb jejich zabezpečení. Stěžejní výstup práce představuje komplexní návrh zabezpečení modelového objektu, zpracovaný na základě realizace bezpečnostního posouzení.

Klíčová slova: poplachový zabezpečovací a tísňový systém, fyzická ochrana, bezpečnostní posouzení, elektronická kontrola vstupu, komunikační prostředky.

ABSTRACT

This diploma thesis deals with the problems of securing the premises of universities, characterizes the specific characteristics of selected areas in terms of their security needs, including the analysis of the requirements of relevant legal and technical regulations in the given area. The aim of the thesis is also the treatment of a description of modern technologies for securing specific areas of universities. The diploma thesis deals with the comparison of the outlined areas in the affected premises in terms of their security needs. The main output of the work is a multifaceted security proposal of the modelled premises, processed on the basis of the implementation of the security assessment.

Keywords: alarm system – Intrusion and hold-up system, physical protection, security assessment, electronic access control, communication means.

Na tomto místě bych rád poděkoval všem, kteří se podíleli na vzniku této diplomové práce, především svému vedoucímu panu Ing. Janu Valouchovi, Ph.D. za jeho odborné vedení, cenné rady a připomínky, vstřícný přístup a trpělivost, kterou mi poskytoval v celém průběhu vypracování práce. Odborným pracovníkům jednotlivých vysokých škol za ochotu a vstřícnost při konzultacích. Dále chci poděkovat celé své rodině za podporu a toleranci po celou dobu studia.

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

I TEORETICKÁ ČÁST.....	12
1 LEGISLATIVNÍ VYMEZENÍ OBJEKTŮ VYSOKÝCH ŠKOL	13
1.1 ZÁKON O VYSOKÝCH ŠKOLÁCH	15
1.1.1 Vnitřní předpisy	17
1.1.2 Prováděcí předpisy	18
1.2 DÍLČÍ ZÁVĚR	18
2 POŽADAVKY NA ZABEZPEČENÍ OBJEKTŮ VYSOKÝCH ŠKOL	20
2.1 FYZICKÁ OSTRAHA	22
2.2 REŽIMOVÁ OPATŘENÍ	23
2.3 TECHNICKÉ PROSTŘEDKY FYZICKÉ BEZPEČNOSTI.....	23
2.3.1 Systémy PZTS.....	24
2.3.2 Systémy EKV,.....	26
2.3.3 Dohledové video systémy	27
2.3.4 Systémy přivolání pomoci.....	28
2.3.5 Požárně bezpečnostní zařízení	29
2.3.6 Systémy EPS	30
2.3.7 Nouzový zvukový systém	31
2.4 DÍLČÍ ZÁVĚR	32
II PRAKTICKÁ ČÁST	34
3 ANALÝZA VYBRANÝCH OBJEKTŮ VYSOKÝCH ŠKOL.....	35
3.1 UNIVERZITNÍ KAMPUS	36
3.1.1 Charakteristika objektu	36
3.1.2 Perimetrická a plášťová ochrana areálu	36
3.1.3 Organizační a režimová opatření	37
3.1.4 Technické prostředky ochrany	38
3.1.4.1 Ochrana osob a majetku.....	38
3.1.4.2 Požární bezpečnost budovy	39
3.1.5 Charakteristické prostory	40
3.2 UNIVERZITA	40
3.2.1 Charakteristika objektu	41
3.2.2 Perimetrická ochrana.....	41
3.2.3 Organizační a režimová opatření	41
3.2.4 Technické prostředky ochrany	42
3.2.4.1 Ochrana osob a majetku.....	42
3.2.4.2 Požární bezpečnost budovy	43
3.2.5 Charakteristické prostory	43
3.3 SOUKROMÁ VYSOKÁ ŠKOLA	44
3.3.1 Charakteristika objektu	44
3.3.2 Perimetrická ochrana.....	45
3.3.3 Organizační a režimová opatření	45
3.3.4 Technické prostředky ochrany	46
3.3.4.1 Ochrana osob a majetku.....	46
3.3.4.2 Požární bezpečnost budovy	46
3.3.5 Charakteristické prostory	47

3.4	ANALÝZA ZÁKLADNÍCH CHARAKTERISTIK OBJEKTŮ VYSOKÝCH ŠKOL	47
3.4.1	Zhodnocení analýzy	50
3.5	DÍLČÍ ZÁVĚR	50
4	BEZPEČNOSTNÍ POSOUZENÍ MODELOVÉHO OBJEKTU	53
4.1	LEGISLATIVNÍ VÝCHODISKA BEZPEČNOSTNÍHO POSOUZENÍ	53
4.2	CHARAKTERISTIKA MODELOVÉHO OBJEKTU	53
4.3	BEZPEČNOSTNÍ POSOUZENÍ - ANALÝZA RIZIK	54
4.4	CHARAKTERISTIKA METODY ANALÝZY RIZIK	54
4.5	SPECIFIKACE AKTIV	55
4.5.1	Klasifikace aktiv	55
4.6	SPECIFIKACE HROZEB	56
4.6.1	Klasifikace hrozeb	56
4.7	IDENTIFIKACE RIZIK	56
4.8	STANOVENÍ BEZPEČNOSTNÍCH RIZIK	57
4.8.1	Nedostatečná kontrola vstupujících osob, neoprávněný vstup	57
4.8.2	Nefunkčnost technických bezpečnostních prostředků	58
4.8.3	Nedodržování režimových a organizačních opatření	58
4.8.4	Vandalismus, Krádež	59
4.8.5	Útok ozbrojené skupiny / jedince	59
4.9	BEZPEČNOSTNÍ POSOUZENÍ – OSTATNÍ VLIVY	61
4.9.1	Ostatní vlivy – vlivy působící ve střeženém objektu	62
4.9.2	Ostatní vlivy – vlivy působící vně střeženého objektu	64
4.10	ZÁZNAM BEZPEČNOSTNÍHO POSOUZENÍ	65
	Identifikační údaje	65
	Základní informace	65
	Charakteristika objektu	66
	Ostatní požadavky	66
	Závěr 66	
4.11	DÍLČÍ ZÁVĚR	67
5	NÁVRH ZABEZPEČENÍ MODELOVÉHO OBJEKTU VYSOKÉ ŠKOLY	68
5.1	ÚVOD	68
5.2	VŠEOBECNÉ ÚDAJE	68
5.2.1	Identifikační údaje stavby	68
5.2.2	Situace	68
5.3	STUPEŇ ZABEZPEČENÍ, TŘÍDA IDENTIFIKACE, TŘÍDA PŘÍSTUPU	69
5.4	PROSTŘEDÍ DLE ČSN CLC/TS 50131-7, ČSN EN 50 131 – 1	70
5.5	ZÁKLADNÍ TECHNICKÉ ÚDAJE MODELOVÉHO OBJEKTU	71
5.5.1	Rozvodné soustavy	71
5.5.2	Ochrana před úrazem elektrickým proudem	71
5.6	STÁVAJÍCÍ BEZPEČNOSTNÍ TECHNOLOGIE MODELOVÉHO OBJEKTU	71
5.6.1	Stávající PZTS	71
5.6.2	Stávající SKV	72
5.6.3	Stávající dohledový systém	72

5.6.4	Stávající EPS.....	73
5.6.5	Stávající MZS.....	74
5.7	NÁVRH ŘEŠENÍ.....	74
5.8	POPIS TECHNICKÉHO ŘEŠENÍ.....	75
5.8.1	PZTS, SKV.....	75
5.8.2	Dohledový systém.....	77
5.8.3	Dorozumívací systém.....	78
5.8.4	Monitorovací a řídicí systém, grafická nástavba.....	79
5.9	NAVRHOVANÁ ZAŘÍZENÍ.....	79
5.10	KONFIGURACE SYSTÉMU.....	81
5.11	UVEDENÍ DO PROVOZU, SERVIS A ÚDRŽBA.....	82
5.12	DÍLČÍ ZÁVĚR.....	83
6	TRENDY V ZABEZPEČENÍ OBJEKTŮ VYSOKÝCH ŠKOL PROSTŘEDNICTVÍM POKROČILÝCH TECHNICKÝCH PROSTŘEDKŮ.....	84
6.1.1	Dílčí závěr.....	87
	ZÁVĚR.....	88
	CONCLUSION.....	89
	SEZNAM POUŽITÉ LITERATURY.....	90
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....	94
	SEZNAM OBRÁZKŮ.....	95
	SEZNAM TABULEK.....	96
	SEZNAM ROVNIC.....	97
	SEZNAM PŘÍLOH.....	98

ÚVOD

Diplomová práce se zabývá návrhem zabezpečení specifických prostor v rámci objektů vysokých škol. Prostředí vysokých škol je místem, kde se setkávají různé oblasti lidské činnosti. Jsou zde realizovány oblasti vědeckovýzkumné a vzdělávací činnosti, ale také oblast běžných pracovně právních vztahů. Prostředí vysokých škol je také místem setkávání různých generací a různých národností. Prostředí vysokých škol je rovněž místem, kde se setkáváme s různými typy prostor, od hlavních volných vstupních prostor přes běžné kancelářské prostory, včetně zasedacích místností, až po specializovaná výzkumná pracoviště. Objekty vysokých škol jsou všeobecně považovány za otevřené, volně přístupné prostory. Primárním úkolem vysokých škol je poskytnout studentům dostupné informace z příslušného vědního oboru a současně poskytnout dostupné prostředky pro vědeckou a výzkumnou činnost v daném oboru. S tím úzce souvisí technická vybavenost specializovaných pracovišť a jejich ochrana a zabezpečení.

Člověk pro svoji tvůrčí činnost potřebuje mít zajištěnu jistou míru zázemí a bezpečí. V současnosti se tento stav stává stálou nutností všech osob a tento vztah se rozšiřuje také na zabezpečení technického vybavení vysokých škol. Zabezpečení, ochrana majetku a osob zahrnuje mnoho faktorů, které spolu navzájem úzce souvisí, vzájemně se doplňují a podporují. Preventivní a administrativní opatření by měla minimalizovat nežádoucí mimořádné události. Tato opatření (standards, směrnice, havarijní plán, atd.) vedou k jisté připravenosti na tyto události. Každá vysoká škola je tvořena objekty se specifickými vlastnostmi. Objekty jsou vsazeny do bezprostředně přilehlého okolí, mají konkrétní provozní potřeby atd.. Těchto informací lze s úspěchem využít při tvorbě návrhu zabezpečení, doporučení při tvorbě prováděcích provozních režimů a vnitřních provozních předpisů. V současné době jsou nedílnou součástí každého objektu technické prostředky pro jeho bezpečný provoz, vyhrazené požárně bezpečnostní zařízení, jehož součástí jsou systémy EPS (elektrické požární signalizace), NZS (nouzové zvukové systémy). Z hlediska ochrany osob a majetku jsou samozřejmostí prostředky technické ochrany skládající se z poplachových zabezpečovacích a tísňových systémů PZTS, Systémů elektronické kontroly vstupu EKV, dohledových videosystémů, Systémů přivolání pomoci SPP, a také komunikačních systémů. Společně s vyspělými technologiemi pro zabezpečení objektů, ať z pohledu „safety“ nebo „security“, jsou nutností odborní pracovníci facility managementu a soukromých bezpečnostních služeb. Obavy z nedostatků v zabezpečení objektů se nejvíce objevují při opětovných projevech hrozeb z pohledu ochrany osob a majetku, ale také při běžném provozu

budov vysokých škol. Nejčastějším důvodem současného stavu je právě podcenění možných rizikových faktorů, jako je volný pohyb osob a s tím související drobné krádeže, krádeže technického vybavení nebo agrese osamělého jedince. Dalším důvodem je omezený rozpočet v oblasti provozních prostředků vysokých škol.

Cílem této práce je charakterizovat specifické vlastnosti vybraných prostor, analyzovat relevantní právní a technické předpisy v dané oblasti. Stěžejní výstup práce představuje komplexní návrh zabezpečení modelového objektu. Závěr práce je zaměřen na moderní technické prostředky v oblasti zabezpečení vhodné pro použití v objektech vysokých škol.

I. TEORETICKÁ ČÁST

1 LEGISLATIVNÍ VYMEZENÍ OBJEKTŮ VYSOKÝCH ŠKOL

Činnost každé vzdělávací instituce je řízena právními předpisy jak v oblasti pracovně právních vztahů tak v oblasti provozování bezpečných budov. Cílem kapitoly je základní vymezení těchto předpisů, podle kterých se řídí každé vysokoškolské zařízení.

Zákon č. 89/2012 Sb.

Nový občanský zákoník ze dne 3. února 2012 s účinností od 1. Ledna 2014 ve znění zákona č. 460/2016 Sb.. Upravuje zejména vzájemná práva a povinnosti osob. Řeší občansko-právní vztahy, ochranu osobnosti a rodiny, upravuje majetková práva fyzických a právnických osob vzájemně a ve vztahu k státu ve vztahu k evropské unii [1].

Zákon č. 262/2006 Sb.

Zákoník práce ze dne 21. dubna 2006 ve znění zákona č. 148/2017 Sb. s účinností od 1. února 2018. Upravuje především pracovně právní vztahy mezi zaměstnavatelem a zaměstnancem, vznik pracovního vztahu, práva a povinnosti pracovníků a zaměstnavatelů. Zabývá se také ochrannou zdraví a při práci [2].

Zákon č. 219/2000 Sb.

Zákon o majetku České republiky a jejím vystupování v právních vztazích ze dne 27. června 2000 ve znění navazujících předpisů upravuje podmínky a způsoby hospodaření a nakládání s majetkem státu, upravuje vystupování státu v právních vztazích a také postavení, zřízení a zánik organizačních složek státu [3].

Zákon č. 218/2000 Sb.

Zákon o rozpočtových pravidlech ze dne 27.června 2000 ve znění zákona č. 367/2017 Sb. a navazujících předpisů upravuje a předkládá pravidla pro nakládání, čerpání a plnění státního rozpočtu. Protože hlavním příjmem do rozpočtu veřejné a státní vysoké školy na vzdělávací a tvůrčí činnost je příspěvek ze státního rozpočtu. Vysoké školy musí tento zákon respektovat [4].

Zákon č. 563/1991 Sb.

Zákon o účetnictví ze dne 12. prosince 1991 ve znění zákona č. 377/2015 Sb. a navazujících předpisů navazuje na předpisy Evropské unie, upravuje způsob vedení a rozsah účetnictví, požadavky na průkaznost a zveřejnění informací z účetnictví [5]. Tyto informace jsou požadovány zákonem č. 111/1998 Sb. o vysokých školách v rámci výroční zprávy o hospodaření předkládané ministerstvu [6].

Vyhláška č. 504/2002 Sb.

Prováděcí vyhláška ze dne 6. listopadu s účinností od 1. ledna 2003 ve znění novely č. 324/2015 Sb., podle které se provádějí některá ustanovení zákona č. 563/1991 Sb. ve znění pozdějších předpisů pro nepodnikatelské subjekty účtující v soustavě podvojného účetnictví [7].

Zákon č. 106/1999 Sb.

Zákon o svobodném přístupu k informacím ze dne 11. května 1999 ve znění zákona č. 205/2017 Sb. s účinností od 1. srpna 2017 ukládá povinnost subjektu poskytnout informace vztahující se k jejich působnosti a rozsahu jejich rozhodovací činnosti a v mezích zákona č. 101/2000 Sb. o ochraně osobních údajů [8].

Zákon č. 309/2006 Sb.

Zákon o zajištění dalších požadavků na bezpečnost a ochranu zdraví při práci v pracovně právních vztazích ze dne 23. května 2006 ve znění zákona č. 88/2016 Sb. s účinností od 1. května 2016 zpracovává a navazuje na předpisy Evropské unie. Navazuje na zákoník práce a další požadavky na pracoviště, pracovní prostředí, pracovní postupy. Zabývá se profesními předpoklady odbornou způsobilostí [9].

Zákon č. 183/2006 Sb.

Zákon o územním plánování a stavebním řádu ze dne 14. března 2006 ve znění zákona č. 225/2017 Sb. s účinností od 1. ledna 2018 upravuje mimo věcí územního plánování, jejich úkolů a cílů, také vyhodnocení vlivů na udržitelný rozvoj území, posuzuje možný vliv staveb a stavebních záměrů na životní prostředí. Tento zákon mimo jiné upravuje také stavební řád ve věcech povolování staveb jejich užívání a odstraňování, dohled a zvláštní pravomoci stavebních úřadů. Tento zákon také řeší podmínky pro projektovou činnost, provádění a provedení staveb, a obecné požadavky na výstavbu [10].

Zákon č. 133/1985 Sb.

Zákon České národní rady o požární ochraně ze dne 17. prosince 1985 ve znění zákona č. 225/2017 s účinností od 1. ledna 2017 stanovuje povinnosti ministerstev, správních úřadů, právnických a fyzických osob, postavení a působnost orgánů státní správy ve vztahu k ochraně života, zdraví a majetku občanů před požáry [11].

Vyhláška č. 246/2001 Sb.

Vyhláška ministerstva vnitra o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru ze dne 29. června 2001 Sb. ve znění vyhlášky 221/2014 Sb. vyslovuje požadavky na množství, druhy a způsob vybavení prostor a zařízení prostředky požární ochrany a požárně bezpečnostními zařízeními dle požárně bezpečnostního řešení stavby případně projektové dokumentace ověřené stavebním úřadem [12].

Vyhláška č. 23/2008 Sb.

Vyhláška o technických podmínkách požární ochrany staveb ze dne 29. ledna 2008 ve znění vyhlášky č. 268/2011 Sb. stanovuje technické požadavky požární ochrany pro návrh, provedení a užívání stavby [13].

1.1 Zákon o vysokých školách

Zákon je v České republice považován za základní, všeobecně platné pravidlo, kterému je každý občan povinen se podřídit. Zákonem jsou stanoveny meze základních práv a svobod, určuje rozsah pravomocí a působnost orgánů veřejné moci. Zákony jsou nadřazeny vyhláškám a nařízením vlády, ale musí respektovat Ústavu a ústavní zákony. Jestliže jsou zákony v rozporu s ústavním pořádkem, lze zákon nebo jeho část zrušit prostřednictvím Ústavního soudu [14]. Zákon, resp. právní předpis je cílem legislativního procesu a rozhodování orgánů veřejné moci s obsahem právních norem a předem daných pravidel chování. Jde o závazný, písemný dokument publikovaný stanoveným způsobem [15].

Zákon č.111/1998 Sb. schválený parlamentem České republiky dne 22. dubna 1998 o vysokých školách ve znění zákona č.137/2016 Sb. upravuje postavení vysokých škol v České republice. Předkládá základní informace o struktuře vysokých škol a vysokého školství v ČR. Upřesňuje členění vysokých škol, stanovuje orgány vysokých škol, informuje o akreditaci studijních programů a také vymezuje působnost Ministerstva školství, mládeže a tělovýchovy ČR. Dle znění zákona je vysoká škola nejvyšší článek vzdělávací soustavy, se svými vrcholnými centry vzdělanosti, nezávislého poznání a tvůrčí činnosti mají důležitou roli ve vědeckém, kulturním, sociálním a ekonomickém rozvoji. Umožňuje absolventům maturitních oborů si zvýšit kvalifikaci a jako jediná instituce v ČR následně udělit akademický titul. Zákon rozděluje vysoké školy na univerzitní, s vzdělávací činností a vlastním výzkumným programem a neuniverzitní, bez výzkumného programu. Dále pak

na veřejné, soukromé a státní vysoké školy. Určuje, že vysoké školy vystupují jako právnické osoby, jsou tvořeny akademickou obcí vysoké školy a zaručují akademickou svobodu a právo [6]. Zákon o vysokých školách řeší také zřízení veřejných vysokých škol. Zřízení a zrušení vysoké školy stejně, jako název a sídlo, je možné provést pouze zákonem a to pro každou vysokou školu samostatně. Zákonem je také určena samosprávná působnost vysoké školy. Mimo např. určování počtu přijímaných uchazečů o studium nebo tvorby a uskutečňování studijních programů, zajištění kvality vzdělávací a tvůrčí činnosti, organizaci studia sem patří především ustanovení samosprávných akademických orgánů veřejné vysoké školy a povinnost řádného hospodaření a nakládání s majetkem vysoké školy. Samotnou činnost a organizaci veřejné vysoké školy stanovují její vnitřní předpisy vysokých škol. Státní orgány jako např. ministerstva mohou zasahovat do organizace a činnosti vysoké školy jen v mezích zákona a jen zákonným způsobem. §7 popisuje samosprávné akademické orgány (akademický senát, rektor, vědecká rada, umělecká rada, akademická rada, rada pro vnitřní hodnocení, disciplinární komise) a další orgány veřejné vysoké školy (správní rada, kvestor). Další body popisují povinnosti akademického senátu, mezi které patří např. schválení rozpočtu a střednědobý výhled veřejné vysoké školy a kontrola využívání finančních prostředků školy. Akademický senát pak schvaluje vnitřní předpisy fakult a ostatní vnitřní předpisy veřejné vysoké školy.

S působností statutárního orgánu jedná a rozhoduje ve věcech školy rektor, je v čele veřejné vysoké školy ve čtyřletém funkčním období. Může být zastoupen prorektory, ty sám jmenuje nebo odvolává. Je předsedou vědecké rady veřejné vysoké školy.

Zákon dále upřesňuje povinnosti vědecké rady, rady pro vnitřní hodnocení, disciplinární komise, správní rady veřejné vysoké školy a kvestora. Kvestor je zodpovědný za vnitřní správu a hospodaření veřejné vysoké školy. Pro kvestora je rozhodující rozpočet a střednědobý výhled, který nesmí být dle § 18 sestaven jako deficitní. Veřejná vysoká škola hospodaří s vlastním majetkem, který je potřebný a primárně určený k vzdělávací a tvůrčí činnosti. Zákon o vysokých školách ve svém §22 určuje součásti veřejné vysoké školy a člení ji na fakulty, vysokoškolské ústavy, jiná pracoviště pro vzdělávací a tvůrčí činnost případně na účelová zařízení pro kulturní a sportovní činnost, ubytování a stravování nebo k zajištění provozu školy [6].

Na fakultách jsou ustaveny samosprávné akademické orgány (akademický senát, děkan, vědecká nebo umělecká rada, disciplinární komise). Dalším orgánem je tajemník, který je zodpovědný za hospodaření a vnitřní správu fakulty v rozsahu určeném děkanem. Uvedené

orgány jednají za veřejnou vysokou školu v rozsahu potřeb fakulty, a to v oblastech vnitřní organizace fakulty, nakládání s finančními prostředky určenými pro fakultu včetně pracovních právních vztahů. Ve věcech fakulty jedná a rozhoduje děkan, je v čele fakulty ve čtyřletém funkčním období. Může být zastoupen proděkan, které sám jmenuje nebo odvolává. Je předsedou vědecké rady fakulty [6].

Také vysokoškolský ústav vykonává tvůrčí činnost a podílí se na vzdělávací činnosti v rámci akreditovaných studijních programů. Je veden ředitelem, kterého jmenuje a odvolává rektor [6].

Zákon o vysokých školách vymezuje také činnost ministerstva, kterému podléhá registrace vnitřních předpisů veřejné vysoké školy. Je-li vnitřní předpis veřejné vysoké školy v souladu s právními předpisy České republiky, ministerstvo jej zaregistruje. Registrací vnitřní předpis nabývá platnost a je přílohou zákona při zřizování vysoké škol [6].

1.1.1 Vnitřní předpisy

Vnitřní předpis, resp. interní normativní akt je právním předpisem. Jako takový není pramenem práva, přestože má normativní charakter, tvoří jen parapravní systém [16]. Pro jeho vydání není potřeba zákonného zmocnění. Zákonem však můžeme uložit povinnost vnitřní předpis přijmout a zákonem také nařídit povinnost se jím řídit. Interními normativními akty rozumíme: statuty, volební řády, nařízení ministerstev, služební předpisy, interní instrukce, stavovské předpisy, pracovní postupy atd. [17]. Vnitřní předpisy nepřekračují hranice organizace nezasahují například do obchodních podmínek, veřejných soutěží, atd.. Vnitřní předpisy jsou vydávány výkonnými orgány organizace, mohou obsahovat právní normy a jsou závazné pro zúčastněné strany.

Veřejná vysoká škola je dle §17 zákona o vysokých školách povinna přijmout, resp. vytvořit, vnitřní předpis podléhající souhlasu a registraci ministerstva školství, mládeže a tělovýchovy. Vnitřní předpis nabývá platnost registrací ministerstvem. V souladu s vnitřními předpisy veřejné vysoké školy musí být také vnitřní předpisy fakult viz. §33.

Vzhledem k právní povaze soukromých vysokých škol zákon neuvádí výslovný výčet vnitřních předpisů jako u veřejných vysokých škol. Vnitřní předpisy soukromých vysokých škol mimo jiné povinně stanovují, které orgány vykonávají stejné funkce jako u orgánů veřejných vysokých škol dle §41 [6].

1.1.2 Prováděcí předpisy

Prováděcí předpis je právním předpisem určený k upřesnění obsahu zákona. Upřesnění obsahu právní normy je prováděno vyhláškami, které jsou vydávány výkonnými orgány správních úřadů (např. ministerstvo, krajský, obecní úřad), nebo nařízením vlády které vydává vláda s podpisem předsedy a příslušného člena vlády. Podle legislativních pravidel vlády je možné vydat prováděcí předpisy jen se zmocněním zákona a s využitím jen zákonných právních norem. Dále nelze zákonem měnit prováděcí předpisy, ani nařízením vlády měnit vyhlášku. Zákonem však lze dotčené prováděcí předpisy zrušit, ruší-li se ustanovení zákona [14].

V zákoně o vysokých školách je řešení povinností, z tohoto zákona vyplývajících, prováděno prováděcími předpisy (např. Vyhláška č. 277/2016 Sb. o předávání statistických údajů vysokými školami, Nařízení vlády č. 275/2016 Sb. o oblastech vzdělávání ve vysokém školství, Vyhláška č. 343/2002Sb. o postupu a podmínkách při zveřejnění průběhu přijímacího řízení na vysokých školách, atd.) [6].

1.2 Dílčí závěr

Legislativní vymezení objektů vysokých škol zahrnuje širokou oblast právních předpisů. Jejich věcná působnost vymezuje, jaké vztahy normy upravují. Objekty vysokých škol, jsou v současnosti budovány a vybavovány na úrovni, která vyhovuje srovnání s vyspělými výzkumnými ústavami včetně pracovního zázemí, oblastí pracovního prostředí pro zaměstnance a akademické pracovníky ale také pro studenty. Ve srovnání jistě obtojí i vybavenost technologiemi, které slouží pro vědeckou a tvůrčí činnost. Nemalé množství výzkumné činnosti probíhá právě na univerzitách. První část předkládá základní legislativní předpisy, se kterými se při řešení technických nebo pracovně právních otázek můžeme setkat. V České republice je oblast vysokého školství řízena zákonem o vysokých školách. Tento právní předpis je součástí právního řádu České republiky. Zákon ukazuje svoji propracovanost zejména ve vztahu ke zřízení a provozování vysokých škol, a to včetně odkazů na ostatní právní předpisy (prováděcí předpisy, vnitřní předpisy). Prostřednictvím hierarchie právního řádu, resp. ostatních právních předpisů, je zodpovědnost přenesena na vysoké školy a jejich vedoucí pracovníky. Technické řešení objektů vysokých škol z pohledu provozu budov nemá v České republice samostatný právní předpis, prováděcí předpis nebo alespoň metodický standard. Objekty vysokých škol tak podléhají běžné legislativě ve výstavbě, kde nacházíme propracovaný systém právních předpisů (vyhlášky, nařízení vlády).

Zájem o bezpečnost vysokých škol, z pohledu ochrany osob a majetku, se dostává do povědomí až s narůstajícím počtem bezpečnostních incidentů, především v prostorách škol a školských zařízení. Bezpečností ve školách se začíná zabývat mnoho institucí. Jedno z prvních metodických doporučení vydává MŠMT ČR ve vztahu ke „školskému zákonu“

- Č.j.: MSMT-37014/2005-25 Metodický pokyn k zajištění bezpečnosti a ochrany zdraví dětí, žáků a studentů ve školách a školských zařízeních zřízovaných MŠMT ČR,
- Č.j.:MSMT-1981/2015-1 Metodické doporučení k bezpečnosti dětí, žáků a studentů ve školách a školských zařízeních jako minimální standard bezpečnosti.

MŠMT aktivně spolupracuje s „Asociací bezpečná škola z.s.“ jako samostatným, nezávislým, zájmovým a dobrovolným spolkem, činným v oblasti bezpečnosti osob, ochrany měkkých cílů, škol a školských zařízení. Asociace organizuje každoroční konference kde, bezpečnost, technické, finanční možnosti a podmínky škol jsou hlavním tématem. Asociace ve spolupráci s MV ČR na základě reálných zkušeností předkládá metodiku pro aplikaci nové technické normy ČSN 734400 „Prevence kriminality - řízení bezpečnosti při plánování, realizaci a užívání škol a školských zařízení“, do praxe byla zavedena dne 1.9 2016. Dalším subjektem, který vydal doporučující „Pokyny ke stanovení úrovně zabezpečení škol“ je AGA – Asociace Grémium Alarm.

Přestože uvedené metodické pomůcky poskytují celkem komplexní přehled o možnostech fyzické ostrahy, mechanickém zabezpečení, elektronických bezpečnostních systémech a jejich účelné kombinaci, nejsou přímo adresovány objektům ve smyslu zákona o vysokých školách. Bezpečnost všech osob, ale zcela jistě překračuje hranice školského zákona i zákona o vysokých školách, je proto možné z vybraných doporučení vycházet nebo je převzít, případně modifikovat dle konkrétních potřeb nejen pro volně přístupné objekty vysokých škol.

2 POŽADAVKY NA ZABEZPEČENÍ OBJEKTŮ VYSOKÝCH ŠKOL

Současná moderní společnost přikládá zajištění ochrany života, zdraví a majetku na všech úrovních nejvyšší prioritu. Zodpovědnost za zajištění bezpečnosti subjektu však není jen v rukou státu, státních orgánech, ale je přenášena na subjekt samý. Bezpečnost v objektech vysokých škol je často vnímána jako stav, kde rizika z hrozeb, jejichž cílem je způsobit újmu, jsou redukována na přijatelnou úroveň „jen“ právě proto, že se pohybujeme na „akademické půdě“ [18].

Požadavky na zabezpečení objektů vysokých škol vycházejí z potřeb konkrétního ústavu, z dostupných možností bezpečnostního průmyslu a jejich relevantních předpisů. Zřízení komplexního systému bezpečnosti je vázáno na zpracované **bezpečnostní posouzení** objektu. Jeho cílem je vytvoření návrhu bezpečnostního systému pro zvýšení ochrany předmětů zájmu prostřednictvím řízení bezpečnostních rizik. Za předměty zájmu v podmínkách vysokých škol považujeme zejména:

- život a zdraví osob (akademický sbor, zaměstnanci, studenti, návštěvy, zaměstnanci servisních a dodavatelských organizací),
- informace (osobní údaje, vybrané interní předpisy, součinnostní dohody,
- majetek ve správě školy (finanční prostředky, výpočetní technika, technické a technologické vybavení laboratoří, chemické, biologické látky atd.).

Úkolem bezpečnostního posouzení je provést analýzu stávajícího stavu zajištění bezpečnosti, stanovit bezpečnostní rizika a specifikovat kritická místa pro budoucí návrh bezpečnostního opatření, navrhnout způsob a rozsah technického zabezpečení případně doporučit optimalizaci strážních a dozorčích stanovišť fyzické ostrahy [19]

Protože doposud nejsou v rámci vysokých škol vydány platné standardy pro oblast ochrany osob, majetku a informací, které by stanovily požadavky na jednotný, minimální rozsah zabezpečení jednotlivých typů objektů a vybraných prostor na vysokých školách, je nutné při stanovení rozsahu zabezpečení respektovat požadavky platných právních předpisů a technických norem, současně přihlídnout na specifické provozní podmínky, na požadavky konkrétního subjektu a jeho ekonomické možnosti.

V rámci procesu zpracování bezpečnostního posouzení objektů vysokých škol je možné se inspirovat požadavky norem, které jsou primárně určeny školám, školským zařízením a jejich provozovnám, nebo pro veřejné, soukromé i státní subjekty. Využít je jako metodické návody pro snížení a prevenci kriminality v objektech vysokých škol. Tyto normy

např. upravují zásady a návrhy pro snížení rizika kriminality a antisociálního chování v přípravných a realizačních fázích stavebního řešení s ohledem na bezpečnostní opatření a požadavky technických norem pro mechanické a elektronické bezpečnostní prvky [20].

- řada norem ČSN EN 14383, Prevence kriminality – Plánování městské výstavby a návrh budov,
- ČSN 734400 Prevence kriminality – Řízení bezpečnosti při plánování, realizaci a užívání škol a školských zařízení.

Dále lze využít řady metodických doporučení např.: Metodika pro aplikaci nové technické normy ČSN 734400 vydané MV ČR [21], nebo sborník ÚNMZ č.35/2013 Moderní evropský standard zabezpečení zdroj [22]. Všechny zmiňované dokumenty vycházejí z návrhu evropské normy řady CEN/TS 14383 [23].

Bezpečnostní posouzení z hlediska návrhu bezpečnostního systému představuje první krok k odhalení faktorů, které mají vliv na určení rozsahu zabezpečení, na volbu vhodných prvků navrhovaného zařízení, na stanovení optimální kombinace bezpečnostních technologií, režimových a organizačních opatření. Cílem bezpečnostního posouzení je stanovení odpovídajícího stupně zabezpečení dle ČSN EN 50131-1 ed.2. V rámci bezpečnostního posouzení je zpracována analýza rizik jako důležitý nástroj pro stanovení vhodných bezpečnostních opatření. Pomocí tohoto nástroje na základě faktů identifikujeme potencionální hrozby, slabá místa objektu, určíme pravděpodobnost výskytu hrozby, míru rizika. Obsahem musí být také posouzení zabezpečovaných hodnot a zabezpečovaných budov. Doporučený postup identifikace rizik včetně možných metod je uveden v ČSN EN 31010: 2011 Management rizik – techniky posuzování rizik, a doporučení dle TNI 01 0350 Management rizik – Slovník (pokyn 73). Budovu je nutné posoudit z pohledu lokality, režimu provozu, stávajících bezpečnostních opatření, konstrukce budovy a ostatních resp. vnitřních a vnějších vlivů. Doporučený obsah a podrobný výklad jednotlivých položek ostatních vlivů je uveden v ČSN CLC/TS 50131-7 [24]. Je potřebné uvést, že uvedená norma stanovuje třídy prostředí odlišně oproti normě ČSN EN 33 2200-1 ed.2 (Elektrické instalace nízkého napětí-část1: základní hlediska, stanovení základních charakteristik).

Výstupem posuzování je zápis o bezpečnostním posouzení, jeho doporučená forma je uvedena v TNI 334591-1 [25], jako příloha F. Povinnost zpracovat bezpečnostní posouzení vychází z požadavku souladu výsledného systému s řadou norem ČSN EN 50131-x, případně požadavku jiného legislativního předpisu (např. v souvislosti s podmínkami zadává-

ní veřejných zakázek) [19]. Následným krokem je vypracování systémového návrhu, vedoucí k eliminaci bezpečnostních rizik. Prostřednictvím efektivní kombinace fyzické ostrahy, režimových a organizačních opatření a technické ochrany objektu budou na minimální úroveň eliminována možná rizika a hrozby.

2.1 Fyzická ostraha

Fyzická ostraha je považována za jeden ze základních pilířů ochrany majetku a osob. Často s podporou vyspělých bezpečnostních technologií je vykonávána osobou přítomnou na místě. S ohledem na lidský faktor umožňuje vybrat optimální variantu při řešení bezpečnostní situace. Fyzická ostraha v objektech škol může být vykonávána zaměstnanci školy, ale dnes častěji, vyškolenými pracovníky průmyslu komerční bezpečnosti (PKB), na základě pověření z obchodní smlouvy [18]. Obecné požadavky na poskytovatele bezpečnostních služeb v PKB jsou uvedeny v ČSN 761702: 2014, (ČSN EN 15602: 2008 -76 1701). Poskytovatelé bezpečnostních služeb – Fyzická ostraha. Norma předkládá požadavky na správu a nakládání se svěřenými prostředky (klíčové hospodářství, správa přístupových karet), dále doporučení při ochraně objektů (plánování služby, nasazení bezpečnostních pracovníků), požadavky na výstroj, technické vybavení, zdravotní a odbornou způsobilost zaměstnance a dále upřesňuje požadavky na pořadatelskou činnost [26]. Takto vybavení pracovníci nejčastěji zabraňují vnášení nebo vynášení neoprávněných předmětů, kontrolují, případně evidují procházející osoby nebo vozidla, odemykají a uzamykají vstupy do objektů ve stanovenou dobu, hlásí mimořádné události (požár, havárie, úraz,) [18]. Odborná způsobilost pracovníků v PKB musí odpovídat kvalifikačnímu standardu dle „Národní soustavy kvalifikací“ pro profesi „Strážný“ – kód: 68-008-E. Autorizujícím orgánem je Ministerstvo vnitra ČR. Poskytovatel bezpečnostních služeb je u svých pracovníků povinen dle právních předpisů odbornou způsobilost prokázat [27].

Pro zajištění objektů vysokých škol je využívání fyzické ostrahy z časového hlediska jako časově vázané na pracovní dobu, případně jako nepřetržité. Dle rozsahu výkonu je prováděna jako přehledová, dozorová, zásahová, případně aktivní víceúčelová a v místě neozbrojená. Zásah resp. bezpečnostní výjezd je realizován až na základě verifikace události vzniklé z bezpečnostních systémů [28].

2.2 Režimová opatření

Režimová a organizační opatření jsou vnímána jako vnitřní předpisy každé organizace. Bezpečnostní opatření jsou jejich nezbytnou součástí. Jejich cílem je upřesnit způsob a zásady ochrany každého chráněného subjektu vzhledem k jeho významu a důležitosti. Jedná se o souhrn organizačních a administrativních opatření, které stanovují zásady, pravidla, oprávnění např. pohybu osob a jejich kontrolu v prostoru organizace, možnosti vnášení a vynášení předmětů z a do objektu [18]. Kindl o režimové ochraně uvádí že: „*je soubohem organizačně administrativních opatření a postupů směřujících k zajištění požadovaných podmínek pro smysluplnou funkci zabezpečovacího systému a jeho sladění s provozem chráněného objektu*“ [29].

Režimová opatření přes určitá omezení pro uživatele přinášejí preventivní prvky k ochraně daného subjektu. V kombinaci s bezpečnostními systémy přinášejí komplexní ochranu objektů.

2.3 Technické prostředky fyzické bezpečnosti

Technické prostředky jsou v dnešní době nezbytnou součástí ochrany objektů. Jejich úkolem je podpora fyzické ochrany, podpora režimových a organizačních opatření, ztížení podmínek pro protiprávní jednání narušitelů. Jsou implementovány do vícestupňové ochrany (obvodová, plášťová, prostorová, předmětová), vytváříme tak komplexní zabezpečení objektu.

Základním prvkem jsou mechanické zábranné prostředky (ploty, brány, dveře, okna, mříže, atd.), zabraňují snadnému přístupu narušitele do objektu. Jsou zařazeny do jednotlivých bezpečnostních tříd RC1 až RC6 dle ČSN EN 1627 – Dveře, okna, lehké obvodové pláště, mříže a okenice – odolnost proti vloupání – požadavky a klasifikace.

Elektronické bezpečnostní systémy (PZTS, EKV, CCTV, EPS, atd.), zejména poplachové systémy, stále monitorují změny fyzikálních veličin v daném prostoru. Na základě jejich vyhodnocení aktivují optickou, akustickou signalizaci, nebo přenosová zařízení. Přístupové a sledovací systémy podporují identifikaci a řídí přístup osob do objektu. Technické prostředky přispívají ke snížení doby reakce fyzické ostrahy na vzniklou událost. Technologické bezpečnostní systémy přispívají k bezpečnému provozu budov, eliminují možná rizika [18]. Na všechny technické prostředky fyzické bezpečnosti jsou, kromě požadavků z oborových norem, kladeny požadavky z hlediska mechanické a elektrické bezpečnosti. Bezpečnost jednotlivých komponent je, v souladu s právními předpisy, možné považovat

za prvotní kvalitativní předpoklad jakosti [19].

Základní právní předpisy v oblasti bezpečnosti výrobků:

- zákon č.102/2001 Sb. o obecné bezpečnosti výrobků ve znění zákona 183/2017 Sb.,
- zákon č. 265/2017 Sb. kterým se mění zákon č. 90/2016 Sb. o posuzování shody stanovených výrobků při jejich vydávání na trh a zákon č. 22/1997 o technických požadavcích na výrobky a o změně a doplnění některých zákonů ve znění pozdějších předpisů.

Pro oblast elektrických bezpečnostních prvků (zařízení) se dále jedná o upřesňující požadavky vyplývající z:

- nařízení vlády č.118/2016 Sb., o posuzování shody elektrických zařízení určených pro používání v určitých mezích napětí při jejich dodávání na trh,
- nařízení vlády č. 117/2016 Sb. o posuzování shody výrobků z hlediska elektromagnetické kompatibility při jejich dodávání na trh,
- nařízení vlády č. 426/2016 Sb., kterým se stanoví technické požadavky na rádiová a telekomunikační zařízení,
- vyhláška č. 528/2005 Sb. o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky 204/2016 Sb.,
- ČSN EN 50130-4 ed.2 Poplachové systémy – Část 4: Elektromagnetická kompatibilita – Norma skupiny výrobků: Požadavky na odolnost komponentů požárních systémů, poplachových zabezpečovacích a tísňových systémů a systémů CCTV, kontroly vstupu a přivolání pomoci [19].

2.3.1 Systémy PZTS

Poplachový zabezpečovací a tísňový systém (PZTS) je komplexem elektronických a elektromechanických technických prostředků, které řeší ochranu objektu proti neoprávněnému vstupu, vniknutí. Střeženy mohou být areály, objekty, nebo vybrané místnosti. Typická skladba systému PZTS:

- ústředna systému – je naprogramována tak, aby řídila celý systém autonomně, přijímala povely obsluhy a předávala informace o stavech systému, detektorů a ostatních systémových prvků obsluze,
- ovládací a signalizační prvky systému – jedná se o systémové ovládací panely, systémové SW nástroje, akustickou, optickou signalizaci,

- systémové linkové moduly (expandery) – pro připojení různých typů detektorů do systému, moduly komunikují po systémové sběrnici, nebo komunikační sběrnici RS 485 [18].

Systémové požadavky na PZTS, na jejich provedení, vlastnosti, včetně požadavků na návrh, projekci, instalaci a údržbu jsou uvedeny v normách řady ČSN 50 131.

- ČSN EN 50 131-1 ed.2 Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 1: Systémové požadavky,
- ČSN EN 50 131-2 Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 2: Detektory narušení,
- ČSN EN 50 131-3 Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 3: Ústředny,
- ČSN EN 50 131-4 Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 4: Výstražná zařízení,
- ČSN EN 50 131-5 Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 5: Požadavky na bezdrátové propojení zařízení,
- ČSN EN 50 131-6 ed.3 Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 6: Napájecí zdroje,
- ČSN EN 50 131-8 Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 8: Zamlžovací bezpečnostní zařízení/systémy,
- ČSN CLC/TS 50 131-7 Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 7: Pokyny pro aplikace,
- TNI 33 4591-1 Poplachové zabezpečovací a tísňové systémy – Část 1: Návrh systému PZTS – Komentář k ČSN CLC/TS 50 131-7,
- TNI 33 4591-2 Poplachové zabezpečovací a tísňové systémy – Část 2: Montáž PZTS – Komentář k ČSN CLC/TS 50 131-7,
- TNI 33 4591-3 Poplachové zabezpečovací a tísňové systémy – Část 3: Uvedení PZTS do provozu a jeho následný provoz, údržba a servis – Komentář k ČSN CLC/TS 50 131-7,

V době rozvoje elektroniky a elektronické komunikace jsou kladeny vyšší nároky také na bezpečnostní systémy, zejména požadavky na jejich dálkovou správu vzájemně komunikujících prvků a jednotnou správu uživatelů. Přínosem vzdálené správy je optimalizace časových nároků samotného správce systému, bezpečnostního manažera, ale především

servisních organizací, s tím úzce souvisí úspora finančních prostředků majitele bezpečnostního systému. Z pohledu technického řešení tak rostou také požadavky na zabezpečení elektronické komunikace vzdálených správců systému.

2.3.2 Systémy EKV,

Systémy elektronické kontroly vstupu lze popsat jako soubor opatření vedoucí k řízení a evidenci přístupu do zabezpečeného objektu na základě přidělených přístupových práv. Systém elektronické kontroly vstupu je technické zařízení, tvořené libovolným počtem vzájemně propojených systémových prvků. Jeho úkolem je elektronická identifikace entity. Srovnání získaných dat ze vstupních zařízení s daty uloženými v systémové paměti probíhá v řídicí jednotce systému. Na základě shody a předem stanovenými přístupovými oprávněními, systém umožní/neumožní ovládnutí přístupového místa [18]. Systémové požadavky na systémy elektronické kontroly vstupu v bezpečnostních aplikacích (na jejich vlastnosti, provedení, včetně požadavků na návrh, projekci, instalaci a údržbu) jsou uvedeny v normách řady ČSN EN 50 133 a nově normách řady ČSN EN 60839-11.

- ČSN EN 50 133-7 Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích – Část 7: Pokyny pro aplikace,

Platnost výše uvedené normy bude ukončena 13.4. 2018

- ČSN EN 60839-11-1 Poplachové a elektronické bezpečnostní systémy – Část 11-1: Elektronické systémy kontroly vstupu – Požadavky na systém a komponenty,
- ČSN EN 60839-11-2 Poplachové a elektronické bezpečnostní systémy – Část 11-2: Elektronické systémy kontroly vstupu – Pokyny pro aplikace,
- ČSN EN 60839-11-31 Poplachové a elektronické bezpečnostní systémy – Část 31-1: Elektronické systémy kontroly vstupu – Implementace IP interoperability na základě webových služeb – Základní specifikace,
- ČSN EN 60839-11-32 Poplachové a elektronické bezpečnostní systémy – Část 32-1: Elektronické systémy kontroly vstupu – Implementace IP interoperability na základě webových služeb – Specifikace systému kontroly vstupu [19].

Systém kontroly vstupu je restriktivní systém, je určen k zajištění, *kdo může kam a kdy* vstoupit, případně za *jakých* podmínek (požadavek na PIN). Může poskytovat kompletní přehled o pohybu osob v objektu, přítomnosti v konkrétním prostoru. Integrací s ostatními

bezpečnostními systémy (PZTS, CCTV, docházkový systém) získáme efektivní nástroj pro minimalizaci hrozeb v zájmovém objektu.

2.3.3 Dohledové video systémy

Kamerové systémy jsou samozřejmou součástí technických prostředků v oblasti bezpečnostních technologií. Dle znění legislativních předpisů slouží kamerové systémy pro monitorování, rekognoskaci, detekci, identifikaci předmětů v rámci zájmové oblasti. Současné standardy pro návrh kamerových systémů na principu IP technologie se odklání od dřívější skladby uzavřených televizních okruhů (CCTV). Dnešní dohledové video systémy (VSS – video surveillance system) plní stejný úkol s vyšším rozlišením možností monitorovat odkudkoli, nonstop a s možností pokročilých analytických funkcí v rámci snímané scény. Typická skladba dohledového systému:

kamerové vybavení, úložiště (PC server), monitorovací pracoviště (PC klient) zařízení pro účely přenosu obrazu (aktivní prvky, síť ethernet) [30]

systémové požadavky na CCTV a VSS, na jejich provedení, vlastnosti, včetně požadavků na návrh, projekci, instalaci a údržbu jsou uvedeny v normách řady ČSN EN50 132 a řady norem ČSN EN 62676.

- ČSN EN 50132-5-3 Poplachové systémy – CCTV dohledové systémy pro použití v bezpečnostních aplikacích – Část 5-3: Video přenos – Analogový a digitální video přenos,
- ČSN EN 50132-7 ed.2 Poplachové systémy – CCTV dohledové systémy pro použití v bezpečnostních aplikacích – Část 7: Pokyny pro aplikace,

Platnost výše uvedené normy bude ukončena 13.4. 2018

- ČSN EN 62676-1 Dohledové video systémy pro použití v bezpečnostních aplikacích - Část 1: Obecně, Výkonové požadavky na video přenos,
- ČSN EN 62676-2 Dohledové video systémy pro použití v bezpečnostních aplikacích - Část 2: Obecné požadavky, Implementace vzájemné spolupráce IP systémů založených na využití http, REST a na síťových (web) službách,
- ČSN EN 62676-3 Dohledové video systémy pro použití v bezpečnostních aplikacích - Část 3: Analogové a digitální video rozhraní,
- ČSN EN 62676-4 Dohledové video systémy pro použití v bezpečnostních aplikacích - Část 4: Pokyny pro aplikace,

Dohledové systémy přinášejí důležité informace v krizových situacích a relevantní data ve správnou chvíli. Současný rozvoj technologie (vyšší kvalita obrazu, videa, rychlost zpracování, přenosu, pokročilé analýzy obrazu) proměňuje dohledové systémy z forenzního nástroje na proaktivní prvek systému fyzické ochrany [31].

2.3.4 Systémy přivolání pomoci

Systémy přivolání pomoci SPP (Social alarm systems, SAS) jsou systémy vyvinuté pro poskytování 24hodinové pohotovosti ve vztahu k aktivaci poplachu, identifikaci, přenosu signálu, přijetí poplachu a jeho vyhodnocení. Dále k zajištění záznamu a obousměrné hlasové komunikace. Poskytuje jistotu pomoci osobám v případech uvažovaného ohrožení. Především je určen pro monitorování osaměle žijících osob, pro detekci stavů tísně nebo vzniku jiné omezující situace.

Systémové požadavky na SPP, na jejich provedení, vlastnosti, včetně požadavků na návrh, instalaci a údržbu jsou uvedeny v normách řady ČSN EN 50134 [32].

- ČSN EN 50134-1 Poplachové systémy – Systémy přivolání pomoci – Část 1: Systémové požadavky,
- ČSN EN 50134-2 Poplachové systémy – Systémy přivolání pomoci – Část 2: Aktivační zařízení,
- ČSN EN 50134-3 ed.2 Poplachové systémy – Systémy přivolání pomoci – Část 3: Místní jednotka a kontrolér,
- ČSN EN 50134-5 Poplachové systémy – Systémy přivolání pomoci – Část 5: Propojení a komunikace,
- ČSN CLC/TS 50134-7 Poplachové systémy – Systémy přivolání pomoci – Část 7: Pokyny pro aplikace,

Uvedené předpisy se dále odkazují na další řady norem:

- ČSN EN 50136 - Poplachové systémy – Poplachové přenosové systémy a zařízení,
- ČSN EN ISO 3741:2000 - Akustika- Určení hladin akustického výkonu zdrojů hluku pomocí akustického tlaku [32].

Systémy přivolání pomoci svými vlastnostmi překračují možnosti poskytování pomoci osaměle žijících osob. Svojí univerzálností umožňují aplikaci v provozech kde, se pracující osoby nacházejí, v prostorech s možným působením nebezpečných vlivů. Jako příklad lze

uvést bankovní domy, úřady, nemocnice, laboratoře výzkumných ústavů, laboratoře vysokých škol.

2.3.5 Požárně bezpečnostní zařízení

Požárně bezpečnostní zařízení (PBZ) ve smyslu zákona č. 133/1985 Sb. o požární ochraně a navazujících předpisů představuje technické prvky zařízení, na jejichž funkčnosti závisí požární bezpečnost objektu. Požárně bezpečnostní zařízení dle vyhlášky č.221/2014 Sb. o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru (vyhláška o požární prevenci) jsou zařízení pro:

- požární signalizaci (např. EPS, zařízení dálkového přenosu, autonomní požární signalizace, ruční požárně poplachové zařízení, atd.),
- potlačení požáru nebo výbuchu (např. stabilní hasicí zařízení, automatické proti výbuchové zařízení, samočinné hasicí systémy),
- usměrňování pohybu kouře při požáru (např. zařízení pro odvod tepla a kouře, zařízení přetlakové ventilace, kouřová klapka včetně ovládacího mechanismu, kouřotěsné dveře, zařízení přirozeného odvětrání kouře),
- únik osob při požáru (např. požární nebo evakuační výtah, nouzové osvětlení, nouzová sdělovací zařízení, funkční vybavení dveří, bezpečnostní a výstražné zařízení),
- zásobování požární vodou (např. vnější požární vodovod včetně nadzemních a podzemních hydrantů, plnicích míst a požárních výtokových stojanů, vnitřní požární vodovod včetně nástěnných hydrantů, hadicových a hydrantových systémů, nezavodněné požární potrubí),
- omezení šíření požáru (např. požární klapka, požární dveře a požární uzávěry otvorů včetně jejich funkčního vybavení, vodní clony, požární přepážky a ucpávky),
- náhradní zdroje a prostředky určené k zajištění provozuschopnosti požárně bezpečnostních zařízení, zdroje nebo zásoba hasebních látek u zařízení pro potlačení požáru nebo výbuchu a zařízení pro zásobování požární vodou, zdroje vody určené k hašení požárů,
- zařízení zamezující iniciaci požáru nebo výbuchu,

Z toho vyhrazenými druhy jsou: elektrická požární signalizace, zařízení dálkového přenosu, zařízení pro detekci hořlavých plynů a par, stabilní a polostabilní hasicí zařízení, automatické proti výbuchové zařízení, zařízení pro odvod tepla a kouře, požární klapky [12].

Návrh PBZ je nedílnou součástí celkového požárně bezpečnostního řešení stavby a jeho minimální rozsah je dán požadavkem vyhlášky č.221/2014 Sb.. Zpracovat návrh PBZ ve vztahu k PBŘ může osoba oprávněná k projektové činnosti podle zákona č.459/2016 Sb. ve znění pozdějších předpisů [13]. Požadavky na PBZ v objektech řeší soubory legislativních předpisů zejména řada norem ČSN 7308xx – Požární bezpečnost staveb, ČSN IEC 6033x Celistvost obvodu za podmínek požáru, Reakce kabelů na oheň –Rozhodnutí komise 2006/751/ES, dále vyhláška č.23/2008 Sb. ve znění vyhlášky 268/2011 Sb., a ZP č.27/2008 pro určení třídy funkčnosti kabelů a kabelových tras, ČSN EN 60849 Nouzový zvukový systém. Požárně bezpečnostní zařízení spolu s organizačními opatřeními jsou prevencí proti vzniku požáru, vedou ke snížení jeho rozsahu a intenzity, snižují riziko jeho vzniku a jeho následků [33].

2.3.6 Systémy EPS

Systém Elektrické požární signalizace je určen k rychlé detekci a lokalizaci místa požáru a k přenesení této informace k osobám zodpovědným za včasný a účinný zásah. Zařízení EPS je soubor ústředí, hlásičů požáru, přenosových a doplňkových zařízení. Je jedním z vyhrazených požárně bezpečnostních zařízení, sloužící ke zvýšení požární bezpečnosti stavby. V souladu s požárně bezpečnostním řešením stavby ovlivňuje další technologické prvky systému požární bezpečnosti staveb (např. stabilní hasící zařízení, zařízení odtahu tepla a kouře, nouzové sdělovací zařízení) [18]. Systémové požadavky na systémy EPS (na jejich vlastnosti, provedení, včetně požadavků na návrh, projekci, instalaci a údržbu), jsou uvedeny zejména v normách např.:

- řada norem ČSN EN 54-xx Elektrická požární signalizace,
- řada norem ČSN 73 08xx Požární bezpečnost staveb,
- ČSN 34 2710 Elektrická požární signalizace – Projektování, montáž, užívání, provoz, kontrola, servis a údržba,
- ČSN EN ISO 13943 Požární bezpečnost – Slovník,
- vyhláška č.268/2011 Sb. Vyhláška o technických podmínkách požární ochrany staveb.
- vyhláška č.221/2011 Sb. o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru (vyhláška o požární prevenci).

Speciální oblastí systémů detekce požáru je autonomní detekce a signalizace (bytové hlásiče požáru), musí být realizována dle ČSN EN 14604 - Autonomní hlásiče kouře, nebo při-

pojením hlásiče dle ČSN EN 54-xx prostřednictvím systému PZTS dle řady norem ČSN EN 50 131 [18].

Hlavním přínosem systémů EPS je rychlá detekce ohniska požáru, aktivace ostatních PBZ. Společně s nimi jsou systémy EPS nepostradatelným prvkem v oblasti požární prevence a požární bezpečnosti v budovách.

2.3.7 Nouzový zvukový systém

Nouzový zvukový systém je využíván ve veřejných prostorech, úřadech, administrativních centrech, školách. Mnohdy je výhodnější použít v případě nebezpečné situace (např. požár v budově) konkrétní mluvené hlášení. Tuto úlohu dokáže automaticky zajistit evakuační rozhlas propojený se systémem EPS. V prostředí ČR podléhají požadavky na systém evakuačního rozhlasu mimo jiné certifikaci dle:

- EN 54-16 - Elektrická požární signalizace – Část 16: Ústředny pro hlasová výstražná zařízení,
- ČSN EN 60849 – Nouzové zvukové systémy,
- ISO 7240-16 – standart - specifikuje požadavky, zkušební metody a výkonnostní kritéria pro zařízení nouzových zvukových systémů [34].

Požadavky na návrh, instalaci, provoz a údržbu těchto systémů se řídí vyhláškou č. 221/2014 Sb. a vyhláškou č.268/2011 Sb. ve znění pozdějších předpisů. Systém lze provozovat v běžném provozu jako systém místního rozhlasu, všechna poplachová hlášení jsou automaticky spouštěna s vyšší prioritou.

2.4 Dílčí závěr

Vymezení požadavků na technické prostředky pro zabezpečení objektů je popsáno v široké škále oborových norem, standardech, TNI, prováděcích předpisech, které se týkají oblasti běžné výstavby. Realizaci je nutné provést také v souladu s těmito podmínkami.

Jak již bylo uvedeno, v ČR ale není stanovena jednotná koncepce pro zabezpečení objektů vysokých škol. Díky spolupráci mnoha asociací, zejména „Asociace bezpečná škola“, ČAP, AGA a státních institucí MŠMT ČR, MV ČR, ÚNMZ jako organizační složka MPO ČR vznikají metodická doporučení vedoucí k smysluplnému řešení bezpečnosti v objektech škol. Předkládají kompletní metodiku dle ČSN 73 4400, která se vztahuje ke školskému zákonu resp. školám a školským zařízením. Pro objekty vysokých škol je ale možné mnohá doporučení přímo převzít, případně se vybranými inspirovat.

V současnosti je zcela běžné, že objekty většiny vysokých škol v ČR nejsou dostatečně zabezpečené zejména u vstupů a to nejen z hlediska technických prostředků, stavebních a interiérových dispozic, ale i z pohledu režimových opatření a organizace vstupu. Vysoké školy jsou vnímány jako otevřené prostory pro různá setkání, konání mnohých konferencí, pro tvůrčí činnost. Přitom právě režim provozu vstupu je jedním z hlavních požadavků (představ) při tvorbě návrhu zabezpečení objektu. Při tvorbě návrhu bezpečnostních opatření je pak nutné postupovat podle reálných potřeb konkrétního subjektu a zejména jeho finančních možností. Je nutné vzít v úvahu, že potřeba „běžného“ uživatele, je přirozeně volný pohyb, a to nejlépe kdekoli v objektu, že „zodpovědný“ uživatel potřebuje mít jistotu, že má zabezpečeny svěřené pracovní prostředky v pracovně, pokud se nachází mimo, např. v PC učebně nebo laboratoři, že jsou zabezpečeny nebezpečné látky v laboratořích, že při pracovní nehodě, nebo ohrožení bude možné rychle přivolat pomoc atp.. Další skupinou jsou osoby zodpovědné za dodržení bezpečného provozu v objektu (ostraha). Je také potřeba brát v úvahu, že každé bezpečnostní opatření přináší jistá omezení pro samotné uživatele, a proto je nutné celý systém koncipovat funkčně pro všechny skupiny uživatelů. Pomocí bezpečnostních a technologických zařízení je možné dosáhnout celkového přehledu o bezpečnostní situaci v objektu. Technologie různých bezpečnostních systémů a znalost jejich ovládání klade zvýšené nároky na osoby fyzické ostrahy objektu. Nároky na bezpečnostní systémy jsou potom zejména rychlost, přesnost a intuitivní ovládatelnost systému. K dispozici jsou integrační nástroje různých technologií prostřednictvím grafické nástavby. Lze jich využít k integraci instalovaných bezpečnostních technologií. Pracovníci ostrahy objektu tak získají nástroj k efektivní identifikaci bezpečnostního inci-

dentu.

V rámci zajištění vyšší bezpečnosti je vhodné přizpůsobit navrhovaný systém pro možnost připojení, např. k operačnímu středisku městské policie nebo operačnímu středisku krizového centra.

II. PRAKTICKÁ ČÁST

3 ANALÝZA VYBRANÝCH OBJEKTŮ VYSOKÝCH ŠKOL

Tato část práce se zabývá porovnáním vybraných objektů vysokých škol z hlediska jejich základních charakteristik, nalézá společné vlastnosti, rysy jejich objektů a typických prostor. Pro potřebu diplomové práce jsou zvoleny vysoké školy s rozdílným oborovým zaměřením jejich fakult jako samostatných subjektů. Uvedené vysoké školy jsou ve městech, jejichž počet obyvatel je v rozmezí cca. 100tis. - 400tis. [35]. Jednou z vybraných vysokých škol je univerzita zabývající se především humanitními, společenskými, přírodními a medicínskými vědami. Pod kterou, mimo ostatní ústavy a jiná pracoviště, spadá 9 fakult:

- právní fakulta,
- filozofická fakulta,
- pedagogická fakulta,
- ekonomicko-správní fakulta,
- fakulta informatiky,
- fakulta sociálních studií,
- fakulta sportovních studií,
- přírodovědecká fakulta,
- lékařská fakulta

V práci bude charakterizován objekt pro tři zmíněné fakulty, který se nachází v rozsáhlém areálu univerzitního kampusu. Další z vybraných vysokých škol je také zaměřena na přírodovědné a humanitní obory, práce se ale zaměřuje na charakteristiku pracoviště technických oborů. Univerzita je tvořena fakultami:

- fakulta technologická,
- fakulta managementu a ekonomiky,
- fakulta multimediálních komunikací,
- fakulta humanitních studií,
- fakulta logistiky a krizového řízení,
- fakulta aplikované informatiky

a dalšími součástmi jako jsou: univerzitní institut, knihovna, koleje, menza a další výzkumné jednotky a parky. Diplomová práce charakterizuje Fakultu aplikované informatiky. Následující vysoká škola, je na rozdíl od předešlých soukromá. Věnuje se pouze ekonomickým oborům, je provozována v rámci jednoho objektu.

3.1 Univerzitní kampus

Kampus je rozsáhlý soubor mnoha moderních budov s učebnami, laboratořemi, studovnami, knihovnou atd. o rozloze několika hektarů a je umístěn na okraji města. Jeho součástí je společensko-kulturní zázemí (obchody, restaurace, služby, ubytování). Jeho hlavním úkolem je podpora studia, vědecké a výzkumné činnosti, vytvoření zázemí pro tvůrčí činnost.

3.1.1 Charakteristika objektu

Celková koncepce univerzitního kampusu je vnímána jako moderně otevřené pojetí organizace prostoru [36]. Objekt univerzitního kampusu je situován v zastavěné okrajové části města v těsné blízkosti obytných budov, objektů fakultní nemocnice a objektů věznice. Dostupnost je prostřednictvím MHD, případně osobním vozidlem. Univerzitní kampus je tvořen 34. pavilony, které se připojují ke společným komunikačním koridorům. Je složen ze dvou celků, severní a jižní část, na střední dělicí úrovni jsou obě části spojeny lávkou. K hlavním komunikačním koridorům JIH, STŘED pro větší část a SEVER pro druhou část, se kromě pavilonů jednotlivých fakult a ústavů připojují i další společné prostory (děkanát LF, zázemí PF, společné výukové centrum, univerzitní knihovna, fakulta sportovních studií, atp.). Hlavní vstup s recepcí, za kterou se nachází aula, je v úrovni 1.np spojen s komerčním a nákupním centrem lávkou s označením CS. Ostatní vstupy s recepcí do areálu jsou v objektu HV1 a v pavilonech AB22, AB34 a AB35 [37].

3.1.2 Perimetrická a plášťová ochrana areálu

Vzhledem ke poloze areálu a veřejnému prostranství v bezprostředním okolí objektů (veřejné cesty), je realizace celkové perimetrické ochrany mechanickými zábrannými prostředky (ploty, brány) pro zamezení přístupu k pavilonům nemožná. Členitý prostor se vzrostlými ozdobnými keři a stromy mezi pavilony je trvale volně přístupný. Přístupové komunikace, parkoviště, jsou řízeny prostřednictvím automatického závorového systému na RFID zaměstnanecké karty. Závoru je možné ovládat z recepcie, případně z centrálního pracoviště ostrahy objektu. Celý prostor parkoviště je dostatečně osvětlen světelnými zdroji veřejného osvětlení. Vzhledem k volně průchozím koridorům po dobu 24 hod., se celková perimetrická ochrana posouvá na pláště jednotlivých pavilonů. U vstupů jsou umístěny čtečky RFID karet a komunikační tablo dorozumivacího systému s možností přivolat

si doprovod. Samostatný vstup do pavilonů je umožněn pouze uživatelům s platnou RFID kartou.

3.1.3 Organizační a režimová opatření

Pro areál univerzitního kampusu je v rámci správního oddělení zřízen samostatný útvar bezpečnosti a ostrahy. Postavení a úlohu pracovníků ostrahy vymezuje Pokyn pro výkon služby v zajištění a ostraze, vydaný vedoucím útvaru bezpečnosti a schválený ředitelem Správy univerzitního kampusu.

Prvořadým úkolem pracovníků útvaru bezpečnosti je ochrana zdraví a života zaměstnanců, studentů, pracovníků spolupracujících subjektů, návštěv. Pro splnění hlavního úkolu je využíváno pěších (Segway) pochůzek, výstupů z dohledového videosystému a výstupů z bezpečnostních systémů. Služba ostrahy na dohledovém centru je nepřetržitá, je s posilou osob vykonávajících pochůzky v areálu a vykonávající kontrolní činnost na vybraných stanovištích (recepcích). Ostraha při plnění úkolů spolupracuje v krizových situacích s techniky správy univerzitního kampusu, případně jednotkami IZS. Pracovníci útvaru bezpečnosti se svojí činností snaží zabránit rozkrádání, ztrátám, poškozování nemovitého i movitého majetku univerzity. K této činnosti využívají technické prostředky střežení, vlastní pochůzkovou a kontrolní činnost. Pracovníci recepcí ve spolupráci s dohledovým centrem zabraňují neoprávněnému vstupu, výstupu osob nebo neodůvodněnému vjezdu, výjezdu vozidel do prostoru univerzitního kampusu nebo parkoviště pro zaměstnance. Dále vedou evidenci jednotlivců nebo skupin osob, které nejsou kmenovými zaměstnanci, vstupují do areálu, vykonávají činnost spolupracujících subjektů. Pracovníci dohledového centra jsou zodpovědní za nepřetržitě vyhodnocování a obsluhu technických prostředků bezpečnostních systémů. Dále monitorují, zda nedochází k závadám na technologických zařízeních, popřípadě předávají informace technické službě. Pracoviště dohledového centra plní funkci ohlašovny požáru. V případě narušení objektu nebo signálu o požáru provede dohledová služba potvrzení příjmu poplachové zprávy a prostřednictvím pochůzkové ostrahy nebo recepčními prověří situaci v místě signalizovaném na panelu bezpečnostního zařízení. Všichni pracovníci bezpečnostního útvaru provedou rozhodný zásah v případě výskytu podezřelých osob vykázaním osoby mimo areál. V případě konfliktu, nerespektování příkazu, podle zhodnocení situace, povolá pracovník ostrahy hlídku Městské policie nebo Policie ČR. V případě požáru, podle závažnosti zjištěného stavu, do příjezdu IZS provádí prvotní zásah nebo zahájí evakuaci osob. Nadále spolupracuje s jednotkami IZS.

3.1.4 Technické prostředky ochrany

Vzhledem k moderní koncepci celého areálu jsou ve všech pavilonech instalovány bezpečnostní technologie jak z pohledu bezpečného užívání budovy, tak z pohledu ochrany osob a majetku. Jejich instalace je v souladu s legislativními předpisy s platnými v době realizace konkrétního pavilonu.

Pro analýzu zabezpečení v objektu je vybrán jeden z typických pavilonů areálu. Objekt je řešen jako trojfrakt s centrální chodbou a atriem se schodištěm, v zadní části pavilonu je centrální chodba ukončena venkovním schodištěm. V podzemní části se nachází technické zázemí (rozvodny, strojovna vzduchotechniky, sklady laboratoře, hygienické zařízení). V 1.–3. n.p. jsou umístěny laboratoře, pracovny, denní místnosti, zasedací místnosti.

3.1.4.1 Ochrana osob a majetku

Ochrana osob a majetku v objektu je podporována poplachovým zabezpečovacím a tísňovým systémem, je řešen podle pravidel pro navrhování a montáž systémů PZTS.

Ochrana objektu proti vnějšímu narušiteli je řešena plášťovou i prostorovou ochranou. Všechny přístupné otvíravé plochy do úrovně 1.np (okna, dveře) jsou vybaveny magnetickými kontakty. Za prosklenými plochami ve stejné úrovni jsou instalovány tzv. audiodektory reagující na zvuk tříštění skla. Prostory navazující na plášťovou ochranu a vybrané kanceláře, chodby, laboratoře, učebny, jsou osazeny prostorovými detektory. Prostřednictvím HW odlišných tísňových tlačítek systému PZTS je realizován systém přivolání pomoci v nouzi pro tělesně postižené spoluobčany, který je instalován na WC a ve sprše. Systém je ovládán prostřednictvím instalovaných ovládacích panelů u jednotlivých střežených oblastí, nebo z aplikace nadstavbového systému instalovaného v prostoru centrálního dispečinku.

Pro zamezení vstupu neoprávněných osob do vybraných prostor je instalován bezkontaktní systém elektronické kontroly vstupu, umožňuje však, předem definovanému okruhu oprávněných osob (návštěva), vstup z veřejných do vybraných prostor v předem vymezených časových intervalech. Instalovaný systém splňuje požadavky třídy přístupu a třídy identifikace a je implementován do univerzitního systému EKV jako celku. Neoprávněné otevření dveří, pokus o sabotáž, překročení doby otevření dveří atd. je automaticky zobrazeno v nadstavbovém systému bezpečnostních technologií.

Cílem dohledového video systému je monitorovat a dokumentovat děje v zájmových oblastech, střežených a rizikových prostorech, zjednodušit a zefektivnit činnost ostrahy (vi-

zuální ověření příčiny poplachového stavu bezpečnostních technologií apod.). Venkovní kamery trvale monitorují plášť budovy v úrovni 1.np, a na střeše přístup a klimatizační jednotky. Vnější kamery jsou chráněny proti mechanickým a klimatickým vlivům ve vyhřívaných krytech. Vnitřní kamery slouží jako přehledové pro monitorování pohybu osob v pavilonu. Obrazové signály z jednotlivých kamer, jsou připojeny na vstupy digitálního záznamového zařízení instalovaného v rozvodně každého pavilonu. Přístup na DVR pro zobrazení kamer na pracovišti ostrahy je prostřednictvím technologické datové sítě.

3.1.4.2 Požární bezpečnost budovy

Požární bezpečnost objektu je řešena dle platných legislativních předpisů. Objekt je členěn do požárních úseků, které respektují určení místností v objektu (schodiště + chodby, instalační šachty, rozvodny, strojovny, sklady, laboratoře, pracovny, venkovní schodiště, chráněné únikové cesty) a současně jejich prostorové členění a rozměry. Odolnost stavebních konstrukcí je v souladu s ČSN 730802 (Požární bezpečnost staveb – nevýrobní objekty) a ČSN 730810 (Požární bezpečnost staveb - společná ustanovení). Evakuace osob z jednotlivých požárních úseků je řešena nechráněnými únikovými cestami ústícími do chráněné únikové cesty s východem na volné prostranství v úrovni 1.np a 1.pp. Větrání únikových a chráněných únikových cest je řešeno vzduchotechnickým zařízením s přívodním ventilátorem a uzavírací klapkou se servopohonem. Odvod vzduchu z chráněné únikové cesty je zajištěn přes otvíravou klapku se servopohonem a dorazem v nejvyšším místě schodiště. Ovládání požárních klapek a ventilátorů je prostřednictvím systému EPS. Elektrická požární signalizace a její automatické hlásiče jsou instalovány ve všech požárních úsecích, manuální hlásiče pak v prostoru únikových cest. Systém EPS mimo ovládání a monitorování stavu požárního větrání vypíná běžnou vzduchotechniku, zvukové projekce v přednáškových sálech a zasedacích místnostech, zajistí sjetí výtahové kabiny na úroveň únikové cesty, uvolní výstupní dveře do volného prostranství, zajistí odpojení elektrické energie a spustí nouzový zvukový systém, jehož zesilovače jsou propojeny do celkového systému areálu. Součástí požárně bezpečnostních řešení je také nouzové osvětlení chodeb, které je automaticky spuštěno v případě odpojení objektu od napájení hlavním zdrojem. Vypnutí elektrické energie je možné vypínacími prvky CENTRAL STOP a TOTAL STOP umístěnými na vnitřní zásahové cestě pro požární zásah. Zařízení pro protipožární zásah, mezi které patří min.3m široké přístupové komunikace pro příjezd požární techniky, nástupní plochy, které jsou součástí vnější a vnitřní zásahové cesty, vnější zásobování vodou pro hašení požáru. Na vybraných místech jsou připravena odběrná

místa s hadicovými systémy k provedení prvotních hasebních prací a přenosné hasicí přístroje. Pro zvýšení požární bezpečnosti je v objektu instalováno stabilní hasicí zařízení – vodní pro běžné prostory, - plynové pro rozvodny a vybrané prostory.

Součástí bezpečnostních opatření je efektivní rozmístění bezpečnostních značek a tabulek pro označení směru úniku.

3.1.5 Charakteristické prostory

Na základě obhlídky areálu univerzitního kampusu a jeho pavilonů (34 budov) lze charakterizovat typické prostory a podle typu místnosti navrhnout zabezpečení z pohledu PZTS a EKV. Skupinu společných prostor zabezpečit pláštěovou ochranou, skupinu prostor laboratoří a technických místností údržby vybavit kompletním zabezpečením včetně kontroly vstupu (Tab. 1.).

Tab. 1 Typické prostory - univerzitní kampus

Zájmový prostor		Technologie				
		PZTS	EKV	CCTV	DZ	EPS
Areál	Vnější 24hod volně dostupný (parkoviště)	NE	ANO	ANO	ANO	NE
	Vnitřní 24hod volně dostupný (hlavní vstupy s recepcí, koridory, chodby)	NE	NE	ANO	NE	ANO
Pavilon	Vnější a vnitřní plášť, Vstup	ANO	ANO	ANO	ANO	NE
	Volné prostory pavilonu (chodby, schodiště, WC)	ANO	NE	ANO	NE	ANO
	Kanceláře, Pracovny, Zasedací místnosti, Sklady, Laboratoře, Denní místnost	ANO	ANO	NE	NE	ANO
	Přednáškový sál, Učebny, Seminární místnosti	ANO	ANO	NE	NE	ANO
	Technické místnosti údržby, Rozvodny	ANO	ANO	NE	NE	ANO

Přístupová oprávnění systému EKV zadává bezpečnostní manager univerzitního kampusu na základě schválených jmenných seznamů od vedoucích ústavů. Jedná se o SW nastavení systému EKV pro jednotlivá přístupová místa ve vazbě SW nastavení systému PZTS

3.2 Univerzita

Univerzita, je označení samostatné a samosprávné vysoké školy, která poskytuje nejvyšší stupeň vzdělání v mnoha různých oborech. Poskytuje odpovídající zázemí pro vzdělávací,

ale také vědeckou, všeobecně tvůrčí činnost. Fakulty univerzit jsou v samostatných a samostatně hospodařících objektech.

3.2.1 Charakteristika objektu

Objekt vybrané fakulty je situován nedaleko centra města v bytové zástavbě. Dostupnost objektu je možná prostředky MHD, běžnými dopravními prostředky. Budova je tvořena betonovým skeletem s otvory pro kovové rámy oken a dveří s výplní ze skla. Hlavní vstup je orientován na severní stranu, prostory pro pobyt částečně na východ a převážně na jihozápad. Ostatní vstupy slouží jako služební, zásobovací, nebo technické. Budova je tvořena volně průchozími objekty s kancelářskými prostory, učebnami, laboratořemi. V budově, díky jejímu uspořádání je zajištěno denní osvětlení a současně omezena tepelná zátěž ze slunečního záření.

3.2.2 Perimetrická ochrana

Okolí budovy je členité se vzrostlými stromy a keři, je volně přístupné pro veřejnost, objekt není oplocen ani vymezen jeho perimetr. Objekt je vsazen do městské zástavby bytových domů. V těsné blízkosti u přístupové cesty je parkoviště pro zaměstnance. Vjezd do prostoru parkoviště je prostřednictvím dopravní značky č.B1 – zákaz vjezdu všech vozidel s dodatkovou tabulkou s výjimkou povolen zaměstnancům fakulty a vozidlům HZS. Přístupový prostor a parkoviště je osvětleno světelnými zdroji veřejného osvětlení.

3.2.3 Organizační a režimová opatření

Fyzická ostraha budovy je realizována pracovníky průmyslu komerční bezpečnosti, na základě pověření z obchodní smlouvy. Organizačně podléhají externí firmě. Hlavním úkolem pracovníka vykonávajícího činnost ostrahy je ochrana života a zdraví osob vstupujících do objektu. Pracovník vykonává činnost na stálém pracovišti v uzavřené recepci v úrovni 1.np. Směna je rozdělena na dvě dvanáctihodinové směny vždy pro jednoho pracovníka. Během denní služby plní zaměstnanec SBS funkci recepčního, provádí výdeje klíčů, přístupových karet pro návštěvy, evidenci vstupujících osob, zprostředkuje a přivolá zodpovědný doprovod pro návštěvu. Vykonává dohled nad poplachovými systémy. V případě poplachové události na některém z instalovaných systémů je odeslána zpráva správci objektu. V součinnosti s pracovníkem SBS a po ověření vzniklé události jsou podniknuta nutná opatření k odvrácení narušení, poruchy. V průběhu noční služby a po odchodu všech osob z budovy ostraha provede zastřežení všech částí objektu. Dohledové praco-

viště SBS monitoruje bezpečnostní technologie a vzniklé poplachové signály. Neporušenost venkovního pláště v nočních hodinách je prováděna pochůzkou po příjezdu motorizované hlídky vyslané z dohledového centra. Délka a četnost kontrolní činnosti na plášti budovy je dle rozhodnutí dohledového centra, dle potřeby a dostupných informací. Pracovník ostrahy s příchodem prvního zaměstnance fakulty provede odblokování střežených prostor. Pracovník ostrahy je povinen v případě vzniku signálu požár, jej bezprostředně přijmout potvrzením na ústředně systému EPS, lokalizovat možné ohnisko a potvrdit jej nebo odvolat. V případě potvrzení informovat dohledové pracoviště, ohroženým osobám poskytnout pomoc a dle závažnosti zahájit prvotní hasební kroky, nebo zahájit evakuaci ohrožených osob. Vyčkat příjezdu a být nápomocen při činnosti záchranných složek IZS.

3.2.4 Technické prostředky ochrany

Ve vybraném objektu jsou instalovány systémy elektronických bezpečnostních technologií pro podporu zabezpečení a monitorování prostoru vybraných částí objektu. Z pohledu ochrany osob a majetku PZTS, z pohledu kontroly vstupu osob EKV, pro monitorování volných prostor a pohybu osob systém CCTV. Z hlediska požární bezpečnosti stavby systém EPS s vazbami na vyhrazená požárně bezpečnostní zařízení.

3.2.4.1 Ochrana osob a majetku

V objektu je pro ochranu osob a majetku instalován systém PZTS. Jeho technické řešení je v souladu s legislativními předpisy pro návrh a montáž těchto zařízení. Ochrana objektu proti narušiteli je řešena plášťovou a prostorovou ochranou. Všechny vstupní dveře jsou vybaveny magnetickými kontakty pro monitorování otevření. Prostory v úrovni 1.np a vybrané prostory kanceláří, případně laboratoří nebo učeben jsou vybaveny prostorovými detektory. Celý systém je na úrovni SW nastavení rozdělen podle požadavku do subsystémů a jeho ovládání povoleno jednotlivým uživatelům

Pro zabránění vstupu neoprávněných osob do vybraných prostor je instalován modulární systém elektronické kontroly vstupu. Prostřednictvím SW nastavení umožňuje předem definovanému okruhu osob v předem stanoveném časovém intervalu vstup z veřejných do vybraných prostor. Systém kontroly vstupu, instalovaný na zkoumané fakultě, je propojen do celkového univerzitního systému. Pokus o neoprávněné otevření dveří, pokus o sabotáž nebo překročení časového limitu pro možné otevření dveří, je uložen v historii řídicí jednotky systému EKV.

Dohledový video systém monitoruje a dokumentuje děje v zájmových oblastech bezpro-

středního okolí budovy, střežených a rizikových prostorech uvnitř objektu. Podporují efektivní činnost ostrahy (ověření poplachového signálu). Venkovní kamery jsou chráněny proti klimatickým vlivům a mechanickému poškození kryty s vyhříváním. Vnitřní kamery slouží jako přehledové pro dohled nad volným pohybem osob. Obrazový výstup ze všech kamer je zobrazen v prostoru recepcce u hlavního vstupu, kde je také vyhodnocen a zaznamenán na DVR.

3.2.4.2 Požární bezpečnost budovy

Požární bezpečnost objektu, odolnost stavebních konstrukcí je řešena v souladu s řadou norem ČSN 73xx (Požární bezpečnost staveb). Objekt je rozdělen do požárních úseků podle určení a plochy místností (chodby a schodiště, chráněné únikové cesty, kanceláře, pracovny, laboratoře, strojovny, rozvodny, instalační šachty). Evakuace osob probíhá nechráněnými únikovými cestami které ústí do chráněných únikových cest případně přímo na volné prostranství v úrovni 1.np a 1.pp. Odvod tepla a kouře je řešeno vzduchotechnickým zařízením v nejvyšším místě budovy, je zajištěn otvíravou klapkou se servopohonem. Ovládání systému vzduchotechnických klapek je prostřednictvím systému EPS. Tento systém mimo to zajišťuje uvolnění vstupních dveří na volné prostranství, sjetí výtahové kabiny do přízemí, automaticky je spuštěna akustická signalizace. Zařízení elektrické požární signalizace je soubor technických prvků, v objektu jsou instalovány dva systémy, které jsou vzájemně propojeny výstupy typu NC. Součástí požárně bezpečnostního řešení objektu je také nouzové osvětlení, to je automaticky spuštěno při výpadku elektrické energie. Zařízení pro protipožární zásah, vnitřní a vnější odběrná místa jsou na vytipovaných místech osazena hadicovými systémy a zajištěno zásobování vodou pro hašení požáru. Pro bezpečný provoz budovy, jsou v objektu rozmístěny bezpečnostní tabulky a značky s vyznačením směru úniku.

3.2.5 Charakteristické prostory

Typické prostory v budově fakulty lze zařadit do skupin podobně jako v předchozím areálu univerzitního kampusu. Skupina společných prostor je zajištěna plášťovou ochranou, skupina prostor typu laboratoře a technické místnosti provozu a údržby je kompletně zabezpečena včetně kontroly vstupu (Tab.2.)

Tab. 2 Typické prostory - univerzita

Zájmový prostor		Technologie				
		PZTS	EKV	CCTV	DZ	EPS
Areál	Vnější 24hod volně dostupný (hlavní vstup, parkoviště)	NE	NE	ANO	NE	NE
Budova	Vnější a vnitřní plášť, Vstupy	ANO	ANO	ANO	ANO	NE
	Volné prostory budovy (hlavní vstup s recepcí, chodby, schodiště, WC)	ANO	NE	ANO	NE	ANO
	Kanceláře, Pracovny, Zasedací místnosti, Sklady, Laboratoře, Denní místnost, Menza	ANO	ANO	NE	NE	ANO
	Přednáškový sál, Učebny, Seminární místnost	ANO	ANO	NE	NE	ANO
	Technické místnosti údržby, Rozvodny	ANO	ANO	NE	NE	ANO

Přístupová oprávnění systému EKV jsou SW nastavena ve vazbě na SW nastavení systému PZTS.

3.3 Soukromá vysoká škola

Stejně jako ostatní typy vysokých škol poskytuje nejvyšší stupeň vzdělání, prostor pro tvůrčí a vědeckou činnost. Oprávnění působit jako soukromá vysoká škola je vymezena udělením státního souhlasu Ministerstvem školství na základě stanoviska Akreditačního úřadu. Soukromá vysoká škola je pro svoji činnost povinna zajistit si finanční prostředky – obvykle se zde na rozdíl od veřejných a státních vysokých škol platí školné.

3.3.1 Charakteristika objektu

Budova je majetkem města, byla vybudována na začátku 20 stol., jako školní objekt pro první a druhý stupeň základní školy. V současnosti je objekt využíván jako studijní středisko soukromě vysoké školy a městské knihovny. Charakterizované prostory studijního střediska jsou zde v dlouhodobém pronájmu. Objekt se nachází v blízkosti centra města v městské zástavbě. Objekt je dostupný běžnými dopravními prostředky. Součástí areálu je knihovna, tělocvična, venkovní sportoviště. Jedná se o čtyřpodlažní budovu včetně části obytného podkroví. Skelet budovy je zděný cihlovými bloky s otvory pro dřevěné rámy plných dřevěných dveří a oken s výplní ze skla. Okenní otvory ve sníženém přízemí resp. 1.pp jsou vybaveny bezpečnostními mřížemi (původní realizace, bez certifikace). Hlavní

vstup a chodby jsou orientovány do školního parku severním směrem, ostatní místnosti kanceláří, přednáškových učeben východním a jižním směrem. Ostatní vstupy slouží jako služební, zásobovací nebo zásahové. Pro potřebu školy jsou využívány všechny podlažní úrovně budovy. Jedná se o hlavní a vedlejší vstupy do objektu, kancelářské prostory, technické prostory, posluchárny a učebny s výpočetní technikou. Společné chodby v objektu jsou přerušeny uzamykatelnou bezpečnostní mříží, která tvoří hranici mezi prostory vysoké školy a městské knihovny.

3.3.2 Perimetrická ochrana

Budova je umístěna v členitém, oploceném areálu školního parku se vzrostlými keři a stromy pro možnost odpočinku. Oplocení je přerušeno vjezdovou dvoukřídlovou bránou pro parkování osobních automobilů zaměstnanců a studentů, druhou pro vjezd zásobovacích vozidel. Oba vjezdy slouží jako přístupové a příjezdové cesty vozidel IZS. Regulace vjezdu není ošetřena žádnými dopravními značkami. Parkoviště je přístupné ve stejném časovém úseku jako provoz školy. Přístup na sportoviště je umožněn z přilehlého schodiště ve školním parku.

3.3.3 Organizační a režimová opatření

Objekt je sídlem dvou samostatných subjektů s rozdílným provozním a organizačním režimem a je bez přítomnosti trvalé fyzické ostrahy. Obě organizace mají samostatné hlavní vstupy chráněné mechanickými zábrannými prostředky. V provozní době jsou prostory vysoké školy přístupné široké veřejnosti. Režim provozu resp. odemykání a zamykání objektu je závislý na osobní a hmotné zodpovědnosti zaměstnanců školy, ze které vyplývá povinnost objekt při ukončení činnosti zkontrolovat, elektronicky zabezpečit vybrané prostory a celý objekt uzamknout. Na prvního příchozího pak připadá povinnost zkontrolovat neporušenost vstupních dveří a odblokovat bezpečnostní systém. V případě poplachové události v mimopracovní době je odeslána zpráva s touto informací zodpovědné osobě, která zajistí potřebnou kontrolu objektu a v případě potvrzení narušení přivolá hlídku městské policie, bude jí nápomocna při lokalizaci narušení a její činnosti

3.3.4 Technické prostředky ochrany

Vzhledem k historické povaze objektu a majetkovým vztahům s městem, jsou všechny bezpečnostní prvky financovány ze strany uživatele. Pro snížení rizika z majetkové trestné činnosti jsou instalovány jen do vybraných prostor.

3.3.4.1 Ochrana osob a majetku

V budově je pro ochranu osob a majetku (zejména majetku) instalován systém PZTS. Technické řešení odpovídá požadavkům legislativních předpisů. Ochrana objektu proti narušiteli je řešena prostorovou ochranou v hlavních vstupních prostorech, chodbách a ve vybraných místnostech (kanceláře, PC učebny, technické místnosti, serverovna). Celý systém je rozdělen do zón na HW úrovni ústředny, jeho ovládání je povoleno podle přístupových úrovní uživatelů.

Systém kontroly vstupu pro monitorování pohybu osob v daném prostoru není instalován. Zařízení pro monitorování a dokumentování dějů v areálu školního parku ani budovy není instalováno.

3.3.4.2 Požární bezpečnost budovy

Požární bezpečnost objektu, zejména odolnost stavebních konstrukcí, určení a výměry místností (schodiště, chodby, únikové chodby, kanceláře posluchárny, rozvodny, atp.) svými vlastnostmi odpovídají požadavkům řady norem ČSN 73xx pro požární bezpečnost staveb. Případná evakuace osob je realizována únikovými cestami přímo na volné prostranství. V budově není vybavení elektrickými vyhrazenými požárně bezpečnostními zařízeními (např. EPS, Nouzový zvukový systém, atp.). Pro detekci požáru jsou ve vybraných prostorech s vyšším požárním zatížením instalovány automatické kombinované hlásiče tepla a kouře, které jsou připojeny na vstupy systému PZTS a monitorovány 24 hodin. Objekt je dále vybaven zařízením pro protipožární zásah, na vybraných místech a ve vybraných prostorech jsou rozmístěny PHP. Pro snadnou orientaci v případě mimořádné situace jsou v objektu rozmístěny bezpečnostní značky a tabulky s vyznačením únikové cesty a směru.

3.3.5 Charakteristické prostory

Z analýzy areálu a budovy soukromé školy lze identifikovat charakteristické prostory a na tomto základě navrhnout zabezpečení osob a majetku. V (Tab. 3) jsou přehledně zapísány typické prostory areálu (venkovní areál, hlavní vstup, vedlejší vstupy, společné chodby, kanceláře, posluchárny, specializované učebny s výpočetní technikou) a způsob jejich zabezpečení.

Tab. 3 Typické prostory - soukromá vysoká škola

Zájmový prostor		Technologie				
		PZTS	EKV	CCTV	DZ	EPS
Areál	Vnější 24hod volně dostupný (oplocení)	NE	NE	NE	NE	NE
	Vnitřní dostupný v pracovní době (školní park, parkoviště, hlavní vstup)	NE	NE	NE	NE	NE
Budova	Volné prostory budovy (hlavní vstup, chodby, schodiště, WC)	ANO	NE	NE	NE	NE
	Kanceláře, Zasedací místnosti, Sklady	ANO	NE	NE	NE	NE
	Posluchárny, PC učebny	ANO	NE	NE	NE	NE
	Technické místnosti údržby, Rozvodny	ANO	NE	NE	NE	ANO

3.4 Analýza základních charakteristik objektů vysokých škol

V rámci analýzy základních charakteristik objektů vysokých škol, provedené osobní obhlídky a konzultací s manažery správy jednotlivých budov jsem každý areál, objekt z bezpečnostního hlediska hodnotil podle:

- **umístění subjektu (areálu, budovy)** - dle katastru nemovitostí, okolní situace, orientace budovy, okolní zástavby, blízkosti významných staveb, dostupnosti dopravními prostředky,
- **skladba subjektu (areálu, budovy)** - komplex budov, průchozí stavební objekty, samostatně stojící budova, členění budovy, počet podlaží,
- **konstrukce budovy** - plné zdivo, železobetonová konstrukce, výplně otvorů, otvíravé plochy,
- **vybavenosti budovy** - bezpečnostní systémy, vzduchotechnika, chlazení,
- **účelu budovy** - výzkumná a tvůrčí činnost, administrativní budova, komerční prostory,

- **účel prostoru** - technické místnosti, rozvodny, sklady, přednáškové sály, učebny, kanceláře, pracovny, laboratoře, speciální pracoviště, volné komunikační prostory, společné prostory,
- **přístupnost budovy** - v pracovní době, trvale přístupná budova,
- **ostrahy objektu** - vlastní ochranná služba, externí ochranná služba, bez ochranné služby, počet členů ochranné služby.

Z hodnocení vyplývá, že objekty zvolené pro potřeby analýzy jsou svými specifickými provozními potřebami a podmínkami velmi rozdílné. U stávajících budov, které byly budovány na konci 19.století, je obtížné získat dnešní standard moderních budov, i přesto splňují minimální požadavky na provoz školy (prostor poslucháren, společných prostor, chodeb, únikových cest). V současnosti je ale nutné, čelit dnešním bezpečnostním hrozbám (krádeže, vandalismus, úrazy). Řešením jsou dodatečně instalované bezpečnostní systémy, včetně bezpečnostního značení. V případě rekonstrukcí nebo budování nových vysokoškolských objektů, je využíváno moderních poznatků z oblasti architektury, stavebnictví, technologických zařízení budov. Objekty jsou situovány do území tak, aby splňovaly požadavky urbanistického a architektonického řešení okolí a současně požadavky na oborové zaměření školy, měly zajištěnou snadnou dopravní obslužnost, a jako takové splnily požadavky normativních předpisů na bezpečný provoz budov.

Analyzované objekty z pohledu zabezpečení lze hodnotit podle:

- dobré dopravní dostupnosti
- konstrukce budovy
- absence elektronické perimetrické ochrany,
- pohybu osob bez omezení v běžné pracovní době ve společných prostorech,
- typických skupin prostor (volné komunikační prostory, společné prostory, kanceláře, přednáškové sály, speciální pracoviště, sklady, technické zázemí),
- provozních technologických zařízení (datové sítě, výtahy)
- bezpečnostních systémů (z hlediska ochrany majetku, provozu objektu),

Všechna hodnotící kritéria a výsledky konzultací a obhlídek analyzovaných objektů jsou přehledně znázorněna v (Tab.4).

Tab. 4 Charakteristika objektů

Charakteristika objektů vysoké školy			
Hodnotící kritéria	Univerzitní kampus	Univerzita	Soukromá škola
Umístění subjektu			
Okolní situace	Dopravní stavby, obslužnost	Dopravní stavby, městský park	Školní park
Orientace budovy	Z	S	S
Okolní zástavba	Komerční stavby	Obytné budovy	Městská zástavba
Blízkost významné stavby	Nemocnice, Věznice		Soud , Věznice
Dostupnost	OA, MHD	OA, MHD	OA, MHD
Typ výstavby	21.století	20.století	19.století
Skladba objektu			
Komplex budov	x		
Průchozí stavební objekty	x	x	
Samostatně stojící budova		x	x
Členění budov	Samostatné pavilony	Objekt	Objekt
Počet podlaží	4 - 6	3 - 8	3
Konstrukce budovy			
Plné zdivo	x	x	x
Železobetonová konstrukce	x	x	
Výplně otvorů	kov, sklo	kov, sklo	dřevo, sklo
Otvíravé plochy	kov, sklo	kov, sklo	dřevo, sklo
Účel budovy			
Přednášková činnost	x	x	x
Výzkumná, tvůrčí činnost	x	x	
Administrativní budova	x	x	
Komerční prostory	x		
Účel prostoru			
Technické místnosti	x	x	
Sklady	x	x	
Přednáškové sály	x	x	
Učebny	x	x	x
Kancelářské prostory	x	x	x
Laboratoře	x	x	
Speciální pracoviště	x	x	
Studovny	x	x	
Knihovna	x		
Jídelna	x	x	
Volné komunikační prostory	x	x	x
Společné prostory	x	x	x

Charakteristika objektů vysoké školy			
Hodnotící kritéria	Univerzitní kampus	Univerzita	Soukromá škola
Vybavenost budovy			
Bezpečnostní systémy	PZTS, SKV, CCTV, EPS, NZS	PZTS, SKV, CCTV, EPS	PZTS
BMS	x	x	
Chlazení	x	x	
Vzduchotechnika	x	x	
Přístupnost budovy			
Volně v pracovní době	x	x	x
Trvale volně přístupná	x		
Ostraha objektu			
Vlastní ochranná služba	x		
Externí ochranná služba		x	
Počet členů ochranné služby	6	1	0
Bez ochranné služby			x

Z provedené analýzy pro potřeby určení charakteristického a ideálního typu objektu vysoké školy vyplývá, že jedním z důležitých faktorů je období výstavby nebo rekonstrukce objektu.

3.4.1 Zhodnocení analýzy

Pro vyhodnocení analýzy a její objektivitu by bylo vhodné zvýšit počet vybraných objektů vysokých škol. V případě uvedené analýzy je počet objektů nahrazen oborovou rozdílností a provozním rozsahem analyzovaných objektů.

3.5 Dílčí závěr

Provedenou analýzu objektů vybraných vysokých škol je možné celkově vyhodnotit tak, že požadavky na zabezpečení jsou u každého objektu z důvodu podobných typových prostor velmi podobné. Je požadováno efektivní řešení s cílem maximálního výsledného zabezpečení, jednoduchosti obsluhy, minimálních požadavků na údržbu, nízkých počátečních a provozních nákladů.

Hlavním úkolem bezpečnostních zařízení je podpora při ochraně života a zdraví zaměstnanců, studentů, zaměstnanců servisních organizací před možnými hrozbami havárií, různých stavů nouze (např. únik nebezpečných látek), při běžném provozu budov, nebo při mimořádné události, dlouhodobém působení přírodních vlivů (např. vichřice, déšť, krupobití apod.). V současné době je také nutné brát na zřetel možnost hrozby z útoku teroristic-

ké skupiny nebo ozbrojeného jedince. Samozřejmou součástí je požadavek na ochranu majetku a technického vybavení vysokých škol. Organizační směrnice, jako součást bezpečnostních opatření, vytváří pro ochrannou službu závazné postupy pro řešení vzniklé situace. Řadí ochranou službu do pozice centra pro ohlášení a zajištění bezodkladného řešení vzniklých bezpečnostních incidentů.

Řešení technického zabezpečení vysokých škol jsou ale velmi rozdílná, některá komplexně na vysoké úrovni, některá nedokonalá, až nedostatečná. Celkově lze zhodnotit, že úroveň zabezpečení vybraných vysokých škol technickými prostředky je závislá na finančních možnostech školy. Je velký rozdíl mezi budovami, které jsou ve výstavbě, které procházejí celkovou rekonstrukcí a jsou komplexně řešeny podle současných legislativních předpisů ve výstavbě. Školy, které jsou provozovány ve stávajících případně, pronajatých, nebo historických budovách, jen těžko mohou, a to zejména z finančních důvodů, dosáhnout na minimální standard zabezpečení.

Dalším dílčím závěrem z provedené analýzy je fakt, že systémy zabezpečení v nových budovách jsou z pohledu ochrany majetku řešeny komplexně prostřednictvím systémů PZTS, EKV, CCTV a splňují očekávané požadavky. Z pohledu ochrany života a zdraví osob jsou v objektech instalována zařízení pro bezpečný provoz budov, zejména požárně bezpečnostní zařízení. Tyto systémy umožňují bezpečnou evakuaci osob v případě požárního nebezpečí. V případě „nepožárního nebezpečí“ a potřeby nutné pomoci se ohrožené osoby musí spolehnout na přítomné zodpovědné pracovníky bezpečnostní služby, funkčnost dohledového systému a ostražitost ostražky při jeho sledování. V objektech není standardem žádný systém pro přivolání pomoci. Hrozba nepožárního nebezpečí je přitom stejně reálná. Možnost přivolat pomoc při nehodě nebo havárii v laboratořích (únik chemické látky apod.) je těžko dostupná, situaci je sice možné řešit prostřednictvím mobilního telefonu, ten ale může být také nedostupný. Scénářů nepožárního nebezpečí, které mohou nastat, je jistě mnoho, není však mnoho způsobů, jak alespoň předat včasnou informaci o vzniklé situaci ostražce objektu, která je v danou chvíli nejbližším možným subjektem odpovědným (organizačními směrnici určeným) a schopným zasáhnout nebo pomoci.

Problém s nedostatečným zabezpečením v případě nepožárního poplachu je řešitelný doplněním bezpečnostních systémů např. manuálními tlačítky typu nouze jako součást systému PZTS. Tato tlačítka pro přivolání pomoci mohou být instalována nejen v krizových prostorech, ale také na volně dostupných chodbách. V provázanosti na systém CCTV a v ideál-

ním případě i na komunikační prostředek, může ostraha bezodkladně lokalizovat, ověřit a řídit vzniklou situací. Ochrana života a zdraví je vždy na prvním místě.

4 BEZPEČNOSTNÍ POSOUZENÍ MODELOVÉHO OBJEKTU

Bezpečnostní posouzení je jedním z kroků při tvorbě návrhu technického řešení bezpečnostních systémů. Odhaluje faktory, které ovlivňují rozsah zabezpečení, volbu vhodných bezpečnostních zařízení a jejich kombinaci. Důležitým nástrojem v rámci bezpečnostního posouzení je zpracování analýzy rizik a stanovení ostatních vlivů působících na objekt.

4.1 Legislativní východiska bezpečnostního posouzení

Bezpečnostní posouzení je z hlediska legislativy vázáno k technickým normám pro zřizování bezpečnostních systémů. Výstup, resp. zápis z bezpečnostního posouzení je důležitým podkladem pro návrh technického řešení a pro pojišťovny. Jeho forma je v ČR vymezena zejména normami ČSN 50131-7, TNI 33 4591-1 a směrnicemi pojišťoven. Při posuzování vnějších vlivů je nutné vzít v úvahu aspekty vzniklé uvnitř i vně střeženého objektu, jejich výčet je uveden v příloze D normy ČSN CLC/TS 50131-7:2011 [24].

4.2 Charakteristika modelového objektu

Modelový objekt vybraný pro zpracování bezpečnostního posouzení je smyšlený včetně souvisejících informací. Budova univerzity je situována v katastrálním území Pardubice, Jižní město, mezi ulice Pod Pekárnou a Nad Valy.

Okolí budovy není oploceno a není vymezen perimetr objektu. Bezprostřední okolí budovy je volně přístupné pro veřejnost. Vjezd na parkoviště pro zaměstnance je situován z přilehlé ulice Nad Valy. Povolení k vjezdu a parkování na parkoviště je ošetřeno zákazovou dopravní značkou č.B1 – zákaz vjezdu všech vozidel s dodatkovými tabulkami s výjimkou pro vjezd vozidel IZS a zaměstnanců univerzity. Budova je tvořena betonovým skeletem, otvory jsou vyplněny kovovými rámy oken a dveří s výplní ze skla. Hlavní vstup s recepcí je ze severní strany, pobytové prostory jsou orientovány z východního až jihozápadního směru. Ostatní vstupy na plášti jsou určeny jako služební, pro zásobování, nebo technické. Budova je koncipována jako vzájemně volně průchozí objekty SO B51, SO B52, SO B53, SO B54, SO B55.

Převážně kancelářské prostory jsou v osmipodlažním objektu SO B51. V objektu jsou dva osobní výtahy, které nejsou určeny k evakuaci osob. K tomuto účelu slouží únikové schodiště v severní části objektu. V objektu SO B53 se třemi nadzemními podlažími jsou umístěny učebny a laboratoře pro vědeckou a tvůrčí činnost. V objektech SO B52, SO B53, SO 54 do úrovně druhého nadzemního podlaží jsou situovány posluchárny, laboratoře,

kanceláře, technologické zázemí budovy, menza. Z východní strany objektu je služební vchod, rampa a manipulační prostor pro zásobování. Uvedené prostory mají samostatný vstup. Samostatnými vstupy z východní a západní strany je rovněž vybaven další subjekt, jsou určeny především jako nouzové. Západní strana objektu v úrovni prvního nadzemního podlaží je vybavena spojovacím koridorem kovové konstrukce se skleněným pláštěm do objektu SO B56.

Z hlediska ochrany osob, majetku a bezpečného provozu budovy jsou v objektu instalována modulární zařízení systému pro ochranu majetku, kontrolu vstupujících osob do vybraných prostor a monitorování jejich pohybu. Z hlediska bezpečného provozu jsou instalována vyhrazená požárně bezpečnostní zařízení se všemi vazbami na zařízení odtahu kouře a tepla, výtahy, uvolnění únikových cest. Monitorování bezpečnostních zařízení je realizováno pracovníkem komerční bezpečnosti, pověřením z obchodní smlouvy, v prostoru recepcie u hlavního vstupu. Pracovník rovněž provádí funkci recepčního, dle pověření vydává uložené klíče, případně přístupové karty, provádí dohled nad dodržováním režimových a provozních opatření.

4.3 Bezpečnostní posouzení - analýza rizik

Analýza rizik je procesní a systematická činnost, jejíž podstatou je identifikace hrozeb, odhad pravděpodobného projevení se hrozby a ocenění míry rizika. Na základě míry rizika lze následně jednotlivým rizikům přiřadit hladinu přijatelnosti. Analýzu rizik je možné charakterizovat jako klíčový nástroj, na jehož základě jsou stanovena vhodná opatření (bezpečnostní, organizační, technická, materiální apod.) k řízení rizika.

Při analýze rizik je zohledněna důležitost aktiv (předmětu chráněného zájmu), jejich hodnota, která přímo ovlivňuje velikost ztrát při působení nebezpečných zdrojů rizik. Uvedený přehled aktiv je sestaven výběrem ze širšího souboru relevantních kritických prvků. Analýza identifikuje reálné hrozby, pravděpodobnost jejich výskytu, slabiny aktiva, úroveň a závažnost jejího dopadu na předmět chráněného zájmu [19].

4.4 Charakteristika metody analýzy rizik

Principem použité metody pro hodnocení rizik je identifikace aktiv a hrozeb a jejich následné bodové ohodnocení, které je založeno na kvalifikovaném odhadu. Uvedený přehled aktiv a hrozeb je stanoven vzhledem k aktuální společenské situaci, úrovni poznatků, požadavků normativních, právních předpisů a vývoji situace v oblasti rizik. Vstupní etapou je

sběr dat. V primární fázi se jedná o identifikaci možných aktiv, identifikaci možných hrozeb, klasifikaci podle jejich důležitosti a zranitelnosti a klasifikace identifikovaných hrozeb. V sekundární fázi pak stanovení míry rizika a jeho přijatelnosti [38].

4.5 Specifikace aktiv

Uvedený přehled aktiv představuje systém (instituci) složený ze skupiny lidských zdrojů, prostředků, probíhajících procesů a vztahů mezi nimi. Cílem je definovat všechna aktiva, jejichž omezení, poškození nebo zničení má přímý dopad na systém [38].

Komplexní přehled aktiv je součástí přílohy č. I.

4.5.1 Klasifikace aktiv

Pro potřeby prováděné analýzy rizik je použita klasifikace formou bodového ohodnocení dle jejich důležitosti. Navrhovaná stupnice bodového ohodnocení aktiv podle důležitosti je obsahem (Tab. 5). Klasifikace důležitosti příslušných aktiv při projevení se identifikovaných mimořádných událostí je součástí přílohy č. I.

Tab. 5 Bodové ohodnocení důležitosti aktiv

Aktiva	
Bodové ohodnocení	Důležitost aktiv (D)
0	zanedbatelná
1	malá
2	nízká
3	střední
4	vysoká
5	velmi vysoká

Pro účel klasifikace z hlediska jejich zranitelnosti je použita multikriteriální metoda umožňující identifikovat stupeň jejich odolnosti vůči možným dopadům hrozeb na základě posouzení vlastností aktiv, která mohou být dotčena možným dopadem identifikovaných hrozeb a posouzením stávajících bezpečnostních opatření chránících aktiva. Úroveň stávajícího zabezpečení se posuzuje podle reálné schopnosti jednotlivých bezpečnostních opatření uchovat vlastnosti aktiv [38]. Výsledkem multikriteriálního posuzování dopadů hrozeb na vlastnosti aktiv je stanovení bodové hodnoty zranitelnosti jednotlivých aktiv dle hodnot uvedených v (Tab. 6).

Tab. 6 Bodové hodnocení zranitelnosti aktiv

Zranitelnost	
Bodové ohodnocení	Zranitelnost aktiva (Z)
0	žádná
1	nízká
2	střední
3	vysoká

Klasifikace zranitelnosti příslušných aktiv, je součástí přílohy č I

4.6 Specifikace hrozeb

Přehled identifikovaných hrozeb je členěn dle jednotlivých typů a klasifikován podle pravděpodobnosti jejich výskytu a je součástí přílohy č. I

4.6.1 Klasifikace hrozeb

Pro potřeby prováděné analýzy rizik je z pohledu pravděpodobnosti výskytu, navržena klasifikační stupnice hodnocení hrozeb (Tab. 7)

Tab. 7 Klasifikace identifikovaných hrozeb

Hrozby	
Bodové ohodnocení	Pravděpodobnost hrozby (P)
0	žádná
1	zanedbatelná
2	nízká
3	střední
4	vysoká
5	velmi vysoká
6	jistá

4.7 Identifikace rizik

Výsledné hodnoty míry rizika jsou matematické operace zohledňující pravděpodobnost projevení se hrozby, důležitost a zranitelnost aktiva.

Rovnice 1 Výsledná hodnota rizika

$$\text{Výsledné riziko} = \text{Pravděpodobnost} \times \text{Důležitost} \times \text{Zranitelnost}$$

Hodnoty míry rizika jsou vyjádřeny kvantitativně i kvalitativně. Kvantitativní míra rizika je stanovena v rozmezí hodnot 1 – 90. K těmto hodnotám jsou přiřazeny údaje vyjadřující hodnotu míry rizika kvalitativně. Kvalitativním hodnocením míry rizika se rozumí stano-

vení jeho míry jako „malé“, „střední“ a „vysoké“. Pro zajištění přehlednosti je kvalitativní míra rizika barevně rozlišena a připojeno hodnocení z hlediska jeho přijatelnosti. Vzájemné vztahy mezi kvantitativním a kvalitativním hodnocením je zobrazeno v (Tab. 8) a v příloze I.

Tab. 8 Princip stanovení míry rizika a jeho přijatelnosti

Kvantitativní hodnota míry rizika	Kvalitativní hodnota míry rizika	Barevné označení závažnosti rizika	Přijatelnost rizika
0 – 35	Malé riziko		Přijatelné
36 – 60	Střední riziko		Přechodné
61 – 90	Vysoké riziko		Nepřijatelné

4.8 Stanovení bezpečnostních rizik

V následujících kapitolách bude uveden přehled rizik, která spadají do přijatelnosti rizika.

- přechodné,
- nepřijatelné

Nepřijatelná rizika nelze tolerovat, musí být odstraněna nebo eliminována v nejkratší možné lhůtě prostřednictvím přijetí vhodných bezpečnostních opatření. Přechodnými riziky je možné se zabývat následně až jsou vyřešena rizika nepřijatelná a budou k dispozici potřebné prostředky (např. finanční, technické) [38].

4.8.1 Nedostatečná kontrola vstupujících osob, neoprávněný vstup

Podle provedené analýzy rizik ve vazbě na ochranu života, zdraví a majetku osob v modelovém objektu se jeví jako největší bezpečnostní riziko nedostatečná kontrola vstupujících/přítomných osob v objektu u hlavního vstupu. Ostatní prostory, resp. vstupy, v budově, jsou buď zabezpečené systémem PZTS, nebo průchod osob je kontrolován systémem EKV. S hrozbou nedostatečné kontroly vstupu úzce souvisí bezpečnost ostatních osob a hmotného majetku v budově. Osoby, které jednájí s úmyslem poškodit objekt, vybavení nebo ohrozit na životě přítomné osoby nemají žádnou překážku, která by zabránila jejich konání. Neoprávněný vstup nepovolaných osob do budovy, usnadňuje příležitost překonat ostatní technické prostředky, nebo může mít násilný charakter. Nedostatečná kontrola osob vstupujících do budovy sebou přináší i další komplikace, jako je např. neznalost počtu přítomných osob v budově. Tato skutečnost v případě mimořádné události komplikuje

je práci ostraze i činnost samotných záchranných složek. Přehled v (Tab. 9), podrobně v příloze III.

4.8.2 Nefunkčnost technických bezpečnostních prostředků

Nefunkčnost technických bezpečnostních prostředků, je další hrozbou vyplývající z provedené analýzy. Díky své vzájemné provázanosti vykonávají komplexní ochranu osob a majetku jednak při běžném provozu budovy, ale také při mimořádné události. V případě trvalého výpadku některého ze systémů může dojít k vážným komplikacím např. při evakuaci osob z budovy. Úzce s tím souvisí dodržování předepsaných pravidelných kontrol technického stavu a plné funkčnosti systémů. Přehled (Tab. 9), podrobně v příloze III.

4.8.3 Nedodržování režimových a organizačních opatření

Nedodržování režimových a organizačních opatření jako nedbalostní jednání osob může vést k ohrožení života a zdraví ostatních, úniku, či ztrátě informací, škodám na hmotném i nehmotném majetku. K uplatnění rizika dochází zejména v důsledku nedostatečného plnění pracovních povinností, uplatňováním rutinních činností, nedostatečné kontrolní činností nebo absenci bezpečnostního vzdělávání zaměstnanců. Jako příklad nedbalostního jednání lze uvést:

- nevyužití systémů technického zabezpečení,
- únik, zprostředkování informací, které mohou být atraktivní pro potencionální pachatele (výsledky vědecké činnosti, uskladněné komodity, informace o bezpečnostním opatření,
- porušení stanovených opatření.

V důsledku takového jednání může dojít k:

- vážným zdravotním újmám,
- zvýšení rizika krádeží, vytvoření vhodných podmínek k páčání trestné činnosti,
- poškození budovy nebo jejích částí.

Hrozbu lze snížit prováděním preventivní činností (vstupní a periodická školení, přezkušování zásad BOZP i protipožárních zásad, bezpečnostních opatření. Dalším preventivním opatřením je také důsledná činnost ze strany odpovědných osob. Přehled (Tab. 9), podrobně v příloze III.

4.8.4 Vandalismus, Krádež

Z analýzy dále vyplývá, že dalšími možnými hrozbami jsou vandalismus a krádeže. Vandalismus je typem trestné činnosti, jehož cílem není zcizení majetku (obohacení pachatele), ale jeho poškození nebo zničení. Typickým projevem vandalismu je poškození fasád budov („graffity“), rozbíjení skleněných výplní, výplní stavebních otvorů budov, poškození oplocení apod. Oproti tomu cílem trestné činnosti krádeže, je majetkové zvýhodnění, obohacení pachatele, nejčastěji zcizením snadno zpeněžitelného majetku. Může k tomu docházet i ve spojitosti s předchozími riziky (nedbalost, návštěvy, pracovníci externích organizací, apod). Z pohledu jednoduchosti zpeněžení, jsou nejčastěji zájmovými předměty vybavení kanceláří, výpočetní a zobrazovací technika, vybavení laboratoří, uložený materiál, kovové předměty. Přehled (Tab. 9), podrobně v příloze III.

4.8.5 Útok ozbrojené skupiny / jedince

Za hrozbu pro modelový objekt můžeme považovat možnost útoku ozbrojené skupiny nebo jedince. V nejobecnější rovině lze tento čin označit za teroristický. Obvykle je zaměřen vůči nezúčastněným osobám za účelem dosažení politických, kriminálních nebo jiných cílů. Z pohledu útočníků, teroristů jsou v zájmu především objekty s velkou kumulací osob. V české republice nemívá terorismus náboženský nebo politický podtext, zpravidla se jedná o čin jisté zájmové skupiny nebo jednotlivce, případně narušené osoby. Mezi nejrozšířenější hrozby patří telefonické vyhrožování uložením výbušného nástražného systému, doručení podezřelých zásilek, nebo výhrůžky k poškození zdraví škodlivými látkami. V případě ohrožení (telefonická, jiná výhrůžka) je nutné vždy informovat Policii ČR a přijmout mimořádná bezpečnostní opatření (evakuace všech osob, omezení vstupu, uzavření objektu). Jako důsledek uvedeného činu lze předpokládat především značné materiální škody na budovách a jejich vybavení. Vzhledem k provedené analýze lze stanovit míru rizika na nízkou. Přehled v (Tab. 9), podrobně v příloze III.

Tab. 9 Přehled rizik

Název identifikované hrozby	Název aktiva	Kvalitativní hodnota míry rizika	Přijatelnost rizika
Nedostatečná kontrola vstupujících (vystupujících) osob, Neoprávněný vstup	Zaměstnanci	Střední riziko	Přechodné
	Studenti	Vysoké riziko	Nepřijatelné
	Externí zaměstnanci		
	Návštěvy		
	Zdravotně postižení, imobilní občané	Střední riziko	Přechodné
	Průmyslové vlastnictví, dokumentace		
	Osobní údaje		
	Interní předpisy a nařízení	Vysoké riziko	Nepřijatelné
	Plášť budovy		
	Hlavní vstup		
	Ostatní prostory	Střední riziko	Přechodné
Hmotný majetek			
Nefunkčnost technických bezpečnostních opatření	Zaměstnanci	Střední riziko	Přechodné
	Studenti		
	Externí zaměstnanci		
	Návštěvy		
	Zdravotně postižení, imobilní občané		
	Průmyslové vlastnictví, dokumentace		
	Osobní údaje		
	Interní předpisy a nařízení		
	Plášť budovy		
	Hlavní vstup		
	Ostatní prostory		
Hmotný majetek			
Nedodržování režimových a organizačních opatření zaměstnanci	Zaměstnanci	Střední riziko	Přechodné
	Studenti		
	Externí zaměstnanci		
	Návštěvy		
	Zdravotně postižení, imobilní občané		
	Průmyslové vlastnictví, dokumentace		
Úraz	Zaměstnanci	Střední riziko	Přechodné
	Studenti		
	Externí zaměstnanci		
	Návštěvy		
Neúmyslné poškození	Zdravotně postižení, imobilní občané	Střední riziko	Přechodné
	Hmotný majetek		
Vandalismus, Krádež	Zaměstnanci	Střední riziko	Přechodné
	Studenti		
	Externí zaměstnanci		
	Návštěvy		
	Zdravotně postižení, imobilní občané		
	Průmyslové vlastnictví, dokumentace		
	Osobní údaje		
	Interní předpisy a nařízení		
	Plášť budovy		
	Hlavní vstup		
	Ostatní vstupy		
Hmotný majetek			

4.9 Bezpečnostní posouzení – ostatní vlivy

Součástí standartního bezpečnostního posouzení při návrhu bezpečnostního systému je posouzení existujících fyzikálních a fyzických podmínek místa instalace z pohledu negativního působení uvnitř nebo vně objektu. Při posouzení objektu z hlediska působení ostatních vlivů je hlavním faktorem stavební konstrukce objektu, dispozice objektu a situace objektu v konkrétní lokalitě. Součástí posouzení je popis režimu provozu objektu, místa uložení klíčů, popis stávajícího zabezpečení, místních a správních předpisů. Při zpracování bezpečnostního posouzení je třeba brát v úvahu řadu faktorů, které mohou ovlivnit správnou funkci bezpečnostních systémů. Jako příklad je možné uvést: vytápění, vodovodní potrubí, vzduchotechnické a klimatizační systémy, zdroje světla a elektromagnetického rušení, výtahy, vnější zvuky, zdroje možného průvanu, vliv vnitřního prostředí z hlediska teploty, vlhkosti světelných podmínek apod. [19] .

Modelový objekt je situován v zástavbě obytných budov, je dostupný běžnými dopravními prostředky. Okolí budovy je volně přístupné veřejnosti, budova je bez perimetrické ochrany. Hlavní vchod je ze severní strany budovy, z přilehlého parkoviště pro veřejnost, případně z parkoviště pro zaměstnance. Vjezd na zaměstnanecké parkoviště je omezen dopravní značkou s dodatkovou tabulkou s povolením k vjezdu vozidel IZS. Ostatní vchody do budovy jsou považovány za služební, zásobovací, technické. Budovu tvoří železobetonový skelet s kovovými rámy oken a dveří se skleněnými výplněmi. Koncepce budovy je tvořena jako volně průchozí stavební objekt s učebnami, laboratořemi, kanceláři, technickým zázemím.

Fyzická ostraha objektu je vykonávána pracovníky externí společnosti, s pověřením dle platné smlouvy. Přítomný pracovník (jedna osoba), vykonává kontrolu vstupujících a odcházejících osob do a z budovy, současně s funkcí recepčního. Zprostředkuje doprovod návštěv, jejich evidenci, realizuje výdej klíčů a přístupových karet. V pracovní náplni je také dohled nad instalovanými bezpečnostními technologiemi, včetně povinnosti kontroly místa vzniku poplachové informace a přivolání pomoci.

V modelovém objektu jsou instalovány bezpečnostní technologie pro ochranu osob a majetku. Je řešena kompletní plášťová a prostorová ochrana ve vybraných prostorech. Kontrola vstupujících osob je řešena u zadního vstupu a vstupů do zájmových prostor. Elektronická kontrola u hlavního vstupu není instalována. Instalovaný dohledový systém monitoruje vybrané oblasti, zaznamenává na DVR a zobrazuje obrazový výstup z kamer na monitorech v prostoru recepcie. Z pohledu požární bezpečnosti jsou v objektu instalovány systémy

EPS, které zajišťují prostřednictvím adresných požárních hlásičů včasnou detekci vznikajícího požáru a předávají tuto informaci do místa trvalé obsluhy.

Pro identifikaci vlivů působících uvnitř objektu je zvolena metoda kontrolního seznamu vlivů, který je doplněný o kvantitativní a kvalitativní odborný odhad spolu se stanovením přijatelnosti daného rizika. Hodnoty jsou stanoveny v rozmezí 1 – 90 a k nim přiřazeny kvalitativní hodnoty vlivu „Malý“, „Střední“, „Vysoký“. Vztah mezi kvalitativním a kvalitativním hodnocením je znázorněn v (Tab.10)

Tab. 10 Princip stanovení působení vlivu a jeho přijatelnosti

Kvantitativní hodnota vlivu	Kvalitativní hodnota vlivu	Barevné označení závažnosti	Přijatelnost vlivu
0 – 35	Malý		Přijatelný
36 – 60	Střední		Přechodný
61 – 90	Vysoký		Nepřijatelný

4.9.1 Ostatní vlivy – vlivy působící ve střeženém objektu

V chráněných budovách se setkáváme s mnoha faktory, které mohou negativně ovlivnit funkčnost instalovaných bezpečnostních technologií. Je nezbytné tyto vlivy identifikovat a zamezit jejich působení již při samotném návrhu systému, např. volbou vhodného zařízení, jeho umístění nebo provedení instalace. Tímto lze minimalizovat jejich negativní působení na přijatelné minimum [19].

Kontrolní seznam představuje reálné vlivy, pravděpodobnost jejich výskytu, úroveň a závažnost jeho dopadu na bezpečnostní systémy. Hodnoty míry vlivu jsou stanoveny dle posouzení daného objektu a informací od uživatele objektu.

Výsledky zvolené metody pro posouzení vlivů působících uvnitř objektu jsou uvedeny v (Tab.11)

Tab. 11 Vyhodnocení působení vnitřních vlivů

Název vlivu			Název akti- va	Kvantita- tivní hodno- ta vlivu	Kvalitativ- ní hodnota vlivu	Přijatel- nost vlivu
Vnitřní vlivy	1.1	Vodovodní potrubí	PZTS	12	Malý	Přijatelný
			SKV	12	Malý	Přijatelný
			CCTV	12	Malý	Přijatelný
			EPS	12	Malý	Přijatelný
	1.2	Vytápění	PZTS	12	Malý	Přijatelný
			SKV	12	Malý	Přijatelný
			CCTV	12	Malý	Přijatelný
			EPS	12	Malý	Přijatelný
	1.3	Vývěsní štítky	PZTS	36	Střední	Přechodný
			SKV	18	Malý	Přijatelný
			CCTV	36	Střední	Přechodný
			EPS	36	Střední	Přechodný
	1.4	Výtahy	PZTS	12	Malý	Přijatelný
			SKV	3	Malý	Přijatelný
			CCTV	3	Malý	Přijatelný
			EPS	3	Malý	Přijatelný
	1.5	Zdroje světla	PZTS	3	Malý	Přijatelný
			SKV	3	Malý	Přijatelný
			CCTV	18	Malý	Přijatelný
			EPS	3	Malý	Přijatelný
	1.6	Elektromagnetické rušení	PZTS	18	Malý	Přijatelný
			SKV	12	Malý	Přijatelný
			CCTV	12	Malý	Přijatelný
			EPS	18	Malý	Přijatelný
	1.7	Vnější zvuky	PZTS	3	Malý	Přijatelný
			SKV	3	Malý	Přijatelný
			CCTV	3	Malý	Přijatelný
			EPS	3	Malý	Přijatelný
	1.8	Průvan	PZTS	18	Malý	Přijatelný
			SKV	12	Malý	Přijatelný
			CCTV	18	Malý	Přijatelný
			EPS	12	Malý	Přijatelný
	1.9	Uspořádání skladovaných předmětů	PZTS	36	Střední	Přechodný
			SKV	18	Malý	Přijatelný
			CCTV	36	Střední	Přechodný
			EPS	18	Malý	Přijatelný
1.10	Plané poplachy, lidský faktor	PZTS	36	Střední	Přechodný	
		SKV	36	Střední	Přechodný	
		CCTV	18	Malý	Přijatelný	
		EPS	36	Střední	Přechodný	

4.9.2 Ostatní vlivy – vlivy působící vně střeženého objektu

Pro úplnost uvádím v (Tab.12) základní přehled faktorů podle ČSN CLC/TS 50131-7 včetně kvantitativního a kvalitativního vyhodnocení.

V současnosti se v okolí budovy nevyskytují žádné dlouhodobě ani krátkodobě působící faktory, žádné VF rušení, ani vlivy působící od okolních objektů nebo nepřiměřené klimatické prostředí. Za nejsilnějším vliv tak v současnosti může být považován sluneční svit směrem k paprskům prostorových detektorů. Vhodným umístěním těchto prvků, nebo volbou vhodného typu, lze tento vliv minimalizovat. Některé faktory se v budoucnu mohou měnit, dle situace je nutné přizpůsobit také konfiguraci bezpečnostních systémů.

Tab. 12 Vyhodnocení vnějších vlivů

Název vlivu			Název aktiva	Kvantitativní hodnota vlivu	Kvalitativní hodnota míry vlivu	Přijatelnost vlivu
Vnější vlivy	2.1	Dlouhodobě působící faktory	PZTS	3	Malý	Přijatelný
			SKV	3	Malý	Přijatelný
			CCTV	3	Malý	Přijatelný
			EPS	3	Malý	Přijatelný
	2.2	Krátkodobě působící faktory	PZTS	12	Malý	Přijatelný
			SKV	12	Malý	Přijatelný
			CCTV	12	Malý	Přijatelný
			EPS	12	Malý	Přijatelný
	2.3	Vliv počasí	PZTS	36	Střední	Přechodný
			SKV	3	Malý	Přijatelný
			CCTV	36	Střední	Přechodný
			EPS	3	Malý	Přijatelný
	2.4	VF rušení	PZTS	12	Malý	Přijatelný
			SKV	12	Malý	Přijatelný
			CCTV	12	Malý	Přijatelný
			EPS	12	Malý	Přijatelný
	2.5	Sousední objekty	PZTS	3	Malý	Přijatelný
			SKV	3	Malý	Přijatelný
			CCTV	3	Malý	Přijatelný
			EPS	3	Malý	Přijatelný
	2.6	Vliv klimatických podmínek	PZTS	3	Malý	Přijatelný
SKV			3	Malý	Přijatelný	
CCTV			3	Malý	Přijatelný	
EPS			3	Malý	Přijatelný	
2.7	Planý poplach, lidský faktor	PZTS	36	Střední	Přechodný	
		SKV	18	Malý	Přijatelný	
		CCTV	18	Malý	Přijatelný	
		EPS	18	Malý	Přijatelný	

4.10 Záznam bezpečnostního posouzení

Záznam bezpečnostního posouzení je výstupem z provedené analýzy rizik a posouzení vnitřních a vnějších vlivů. Doporučená forma je předložena v TNI33 4591-1 Návrh systému, v příloze F jako dotazníkový formulář. Je doporučeno tento zápis mít podepsaný všemi zúčastněnými stranami (zákazník, zástupce dodavatele, zástupce pojišťovny, zástupce provozovatele DPPC) [25]

Záznam uvedený v této práci neobsahuje nevyužité položky v dotazníkovém formuláři v dle TNI 33 459 – příloha F.

BEZPEČNOSTNÍ POSOUZENÍ

Identifikační údaje

Název objektu:	Budova U55, Fakulta elektrotechniky a automatizace
Adresa objektu:	Univerzita Pardubice, Fakulta elektrotechniky a automatizace Pod Pekárnou 1145, 560 07 Pardubice, Česká republika
Investor:	Univerzita Pardubice, Nad Valy 630, 560 05 Pardubice, Česká republika
Zhotovitel BP:	OFFLINE spol.s r.o. U sudu 15, 369 02 Příbram

Základní informace

- Nekomerční objekt: budova vysoké školy
- Vztah k objektu: vlastník
- Chráněný majetek: budova, vybavení budovy, výpočetní a audiovizuální technika, měřicí přístroje, vybavení laboratoří, interní informace, osobní údaje.
- Hodnota max. odhad: 350 mil. ,-Kč
- Poloha objektu: hromadná zástavba
- Historie vloupání: není známo,
v blízkém okolí: není známo

Charakteristika objektu

- Umístění zabezpečovaných prostor: vícepodlažní objekt
- Konstrukce objektu: železobetonový skelet s vyzdívkami z cihelných bloků
- Konstrukce příček: zděné / sádrokartonové
- Vstupní dveře: kovové, prosklené, protipožární
dveřní mechanismus: jednoúčelový, mechanický, s el.mag. otvíračem
klíče: mechanické
- Okna: kovová, skleněná výplň, bez folie, bez mříží
- Ostatní otvory: ventilace, světlíky, technologické otvory

Ostatní požadavky

- Požadavky: ČSN 50131, stupeň zabezpečení: 2 / vybrané prostory 3, pomoc v tísni
- Požární ochrana: EPS
- Ostatní záznamy

Závěr

- PZTS: st. Zabezpečení 2 / vybrané místnosti 3, pomoc v tísni
- Požární signalizace: EPS

Zapsáno: v Pardubicích, 4.dubna 2018

Posouzení provedl: podpis:

Zástupce investora: podpis:

Zástupce pojišťovny: podpis:

Provozovatel DPPC: podpis

4.11 Dílčí závěr

Bezpečnostní posouzení objektu se věnuje identifikaci hrozeb, jejich pravděpodobnosti uplatnění, hodnotám aktiv a stanovuje míru a přijatelnost rizika. Dále se věnuje popisu stavebního řešení objektu, vlastnostem konstrukce budovy, jejímu umístění vzhledem k okolnímu prostředí. V tabulce předkládá rizikové faktory a hrozby, které mohou nastat. I přesto, že jsou v objektu instalována bezpečnostní zařízení, je kontrola vstupujících osob do objektu nedostatečná. Jedná se o závažnou hrozbu, jejímž následkem může být pronešení nebezpečných předmětů a následné ohrožení ostatních osob v objektu. S tím souvisí hrozba neoprávněného vstupu osob, s úmyslem zcizit nebo poškodit zařízení nebo vybavení budovy. Ostraha objektu, přestože je v pracovní době trvale přítomna na pracovišti, nemá možnost identifikovat vstupující/odcházející osoby, nebo v případě mimořádné události efektivně zjistit přesné místo incidentu ohrožených osob ani jejich přesný počet v objektu a umožnit tak, rychlou a účinnou evakuaci osob. Rizikový je také výkon služby v počtu jedné osoby, v případě jakékoli události je přítomná služba povinna provést verifikaci v místě vzniku. Není pak schopna řešit jiné povinnosti, události. Není také splněna nutnost trvalé obsluhy v místě ohlašovny požáru.

Výše uvedené hrozby jsou nepřijatelným rizikem a je nezbytné je eliminovat vhodnými opatřeními, např.:

- doplnění kontroly vstupu na ostatní vstupy do budovy,
- doplnění dohledového systému na plášti a hlavních chodbách budovy,
- vybudování kontrolního místa u hlavního vchodu,
- regulace a kontrola průchodu všech osob u recepcce,
- doplnění systému PZTS o nouzové přivolání pomoci,
- zavedení integrace, vizualizace bezpečnostních systémů.

Eliminací hrozeb u vstupů bude zajištěna vyšší úroveň bezpečnosti osob nacházejících se ve vnitřních prostorech budovy. Další zvýšení úrovně ochrany všech osob bude zajištěno rozšířením instalace PZTS o tísňové hlásiče a monitorováním kritických míst dohledovým systémem. Pro efektivní činnost ostrahy objektu v krizových situacích bude doporučeno instalovat integrační a vizualizační SW.

5 NÁVRH ZABEZPEČENÍ MODELOVÉHO OBJEKTU VYSOKÉ ŠKOLY

Návrh zabezpečení modelového objektu vysoké školy, který je zpracován v této kapitole, vychází ze zpracovaného bezpečnostního posouzení na fiktivní objekt univerzity v Pardubicích. Jako modelový objekt byla zvolena budova U55 jako jeden z objektů Univerzity Pardubice.

5.1 Úvod

Navrhovaná technická řešení bezpečnostních technologií jsou technologickou rekonstrukcí stávajících bezpečnostních systémů.

Návrh skladby systémů je výstupem první etapy v procesu zřizování technologií pro zabezpečení objektu. Návrh slouží především jako pomocný dokument při jednání s investorem, uživatelem, je možné jej modifikovat dle doplňujících informací nebo požadavků a potřeb zúčastněných stran. Veškeré změny musí být smluvními stranami potvrzeny podpisem a řádně zadokumentované.

5.2 Všeobecné údaje

Objednatelem návrhu systému bezpečnostních technologií je Univerzita Pardubice. Objednává návrh komplexního technického řešení (rekonstrukci) bezpečnostních systémů v objektu U55 Fakulty elektrotechniky a automatizace pro zvýšení bezpečnosti studentů, zaměstnanců a majetku, zajištění vyšší kontroly pohybu osob v objektu, optimalizaci obsluhy bezpečnostních systémů uživatelem, zefektivnění činnosti ostrahy.

5.2.1 Identifikační údaje stavby

Adresa objektu:

Univerzita Pardubice - Fakulta elektrotechniky a automatizace,

Pod Pekárnou 1145,

560 07 Pardubice, Jižní město

Česká republika

5.2.2 Situace

Objekt je situován v katastrálním území Pardubice, Jižní město mezi ulice Pod Pekárnou a Nad Valy. Je využíván pro Fakultu elektrotechniky a automatizace (FEA), Fakultu tech-

nologickou (FT), Ústav tělesné výchovy a Menzu. Perimetr objektu není nijak vymezen, plášť budovy je volně přístupný pro veřejnost. Koncepce budovy je řešena z vzájemně volně průchozích stavebních objektů SO B51, SO B52, SO B53, SO B54, SO B55. V hlavní budově SO B51 s osmi podlažimi jsou umístěny převážně kancelářské prostory, v části SO B53 se třemi podlažimi jsou specializovaná pracoviště, odborné učebny, posluchárny, a části SO B52, SO B54, SO B55 dosahují úrovně druhého nadzemního podlaží s technologickým vybavením a zázemím budovy, menzou. Budova je v částech SO B51 vybavena dvěma osobními a v části SO B53, B54 jedním osobním a jedním nákladním výtahem (nejsou určeny k evakuaci osob). Hlavní vstup s recepcí je orientován severním směrem. Z východní strany budovy jsou: služební vchod, manipulační rampa, manipulační prostor pro zásobování budovy, dále trafostanice, laboratoře pro zpracování polymerů a kotelny. Všechny tyto prostory mají samostatné vstupy. Další samostatné vchody jsou pro Ústav tělesné výchovy a to z východní i západní strany budovy. Spojovacím koridorem je přístup do Přírodovědeckého parku v budově U55/156. Z pohledu volného průchodu osob v bezprostředním okolí objektu není objekt oplocen. Oplocení nebylo instalováno z důvodu znění vyhlášky č. 268/2009 Sb. ve znění vyhlášky č. 323/2017 Sb. o technických požadavcích na stavby §7, kdy oplocení nesmí svým rozsahem a použitým materiálem narušit charakter stavby nebo jejího okolí.

5.3 Stupeň zabezpečení, třída identifikace, třída přístupu

Stupeň zabezpečení pro zvolený modelový objekt je na základě bezpečnostního posouzení stanoven na stupeň zabezpečení 2 (nízké až střední riziko). Předpokládá se, že narušitel má minimální znalosti o bezpečnostních systémech a má k dispozici základní nářadí [24]. Stanovení úrovně ochrany podle ČSN EN 60839-11-1 ve vztahu k systému kontroly vstupu a jeho komponent, včetně požadavku např. na monitorování a aktivaci přístupových míst, rozpoznávání, signalizaci nátlaku apod. stanoven na stupeň 2 (nízké až střední riziko - kanceláře, malá firma, škola) [39].

5.4 Prostředí dle ČSN CLC/TS 50131-7, ČSN EN 50 131 – 1

Třída prostředí pro prvky bezpečnostních systémů byla určena dle jejich předpokládaného umístění. Podle uvedených norem rozlišujeme čtyři třídy prostředí. Třída prostředí I. vnitřní (obytné prostory, stálá teplota), třída prostředí II. vnitřní všeobecné (výrobní haly, sklady, garáže), třída prostředí III. venkovní chráněné prvky jsou chráněny např. povětrnostními kryty (ovládací panely, čtečky bezkontaktních karet např. u hlavního vstupu), třída prostředí IV. Venkovní všeobecné zařízení lze plně vystavit povětrnostním vlivům (akustická – optická signalizace, kamery) podrobně v (Tab.13)

Tab. 13 Třídy prostředí přehled

Třída prostředí	Název prostředí	Popis prostředí	Rozsah teplot
I.	Vnitřní	Vlivy prostředí vyskytující se obvykle ve vnitřních prostorách při stálé teplotě (např. v obytných nebo obchodních objektech)	+ 5 °C až + 40°C
II.	Vnitřní všeobecné	Vlivy prostředí vyskytující se obvykle ve vnitřních prostorách, kde není stálá teplota (např. na chodbách, v halách nebo na schodištích a tam, kde může docházet ke kondenzaci na oknech a v nevytápěných skladových prostorách nebo skladištích, v nichž vytápění není trvalé).	10 °C až + 40°C
III.	Venkovní chráněné	Vlivy prostředí vyskytující se obvykle vně budov, přičemž komponenty PZTS nejsou plně vystaveny povětrnostním vlivům.	-25 °C až + 50°C
IV.	Venkovní všeobecné	Vlivy prostředí vyskytující se obvykle vně budov, přičemž komponenty PZTS jsou plně vystaveny povětrnostním vlivům.	-25 °C až + 60°C

zdroj [19]

Vnější vlivy pro vnitřní prostory - normální, prostor bezpečný

Vnější vlivy pro vnější prostředí - AA7 (-25°C - +55°C), AB (-50°C - +40°C platí pro prostory nechráněné před sluncem a mrazem), prostor zvláště nebezpečný.

Návrh uvažuje uvnitř objektu s instalací prvků pro třídu prostředí I. a II.(prostředí vnitřní a vnitřní všeobecné) vně objektu s instalací prvků pro třídu prostředí III. a IV (prostředí venkovní chráněné a venkovní všeobecné).

5.5 Základní technické údaje modelového objektu

5.5.1 Rozvodné soustavy

- NN: 3PE N 400V/50Hz TN-C-S,
- provozní 230V/50Hz TN-C-S,
- slaboproudé PZTS 12V_{ss}, SELV,
- slaboproudé SKV 12V_{ss}, SELV,
- slaboproudé CCTV 230V/50Hz,
24V_{st}, SELV.
PoE

5.5.2 Ochrana před úrazem elektrickým proudem

Základní ochrana před úrazem elektrickým proudem resp. nebezpečným dotykovým napětím živých částí je provedena:

- samočinným odpojením od zdroje v síti TN-C-S,
- malým napětím SELV / PELV.

5.6 Stávající bezpečnostní technologie modelového objektu

Na základě obhlídky objektu a konzultací s pracovníky správy budovy byla provedena analýza stávajících bezpečnostních technologií v modelovém objektu budovy U55 Fakulty elektrotechniky a automatizace. Jednotlivé technologie jsou popsány v samostatných kapitolách.

5.6.1 Stávající PZTS

V modelovém objektu je z hlediska ochrany osob a majetku instalován samostatný systém PZTS do stupně zabezpečení 3 v třídě prostředí II, GALAXY 504 pro elektronické zabezpečení objektů dle řady norem ČSN EN 50 131. Je to modulární systém s využitými čtyřmi komunikačními sběrnicemi RS485, připojenými až šestnácti vstupně/výstupními moduly RIO pro osm monitorovaných vstupů a čtyřmi ovládacími výstupy. Na uvedené sběrnici je jsou také připojeny kombinace modulů RIO, ovládacích klávesnic MK 7 nebo modulů pro připojení čteček RFID karet. Moduly jsou umístěny v podhledech na chodbách, technických místnostech, rozvodnách. K instalované ústředně PZTS je na první komunikační lince připojen modul pro datový přenos informací o stavu systému na DPPC SBS. Popla-

chové informace, informace o technickém (porucha, tamper) stavu, jsou zobrazovány na vybraných systémových ovládacích panelech (stálá obsluha, recepce 1.np). Celý systém je SW rozdělen do subsystémů a podle uživatelských potřeb přidělen jednotlivým uživatelům až 100 uživatelů). Každá manipulace se systémem je ukládána do systémové paměti událostí a paměti událostí na DPPC.

5.6.2 Stávající SKV

V modelovém objektu je z hlediska kontroly přístupujících osob instalován systém kontroly vstupů COMINFO. Jedná se o modulární systém tvořený řídicí jednotkou, dveřními jednotkami, čtečkami systému dveřními otevírači, zdroji pro napájení systémových modulů, zdroji pro napájení elektrických otevíračů a záložními napájecími zdroji. Pro potřebu zamezení volného vstupu přichozích osob, jsou u vybraných přístupových míst instalovány čtečky se snímací hlavou L-PRO-WIEGAND, které pracují s frekvencí 125kHz (LF). Řídicí jednotky s vlastním nebo sdíleným zdrojem REI:MP a REA:MP pro až čtyři snímací zařízení, komunikují prostřednictvím ethernetu s centrálním serverem, na kterém běží služby CARDPAY, PASSPORT, ACCESS čerpají ze společné databáze uživatelů. Uživatelské karty typ EM Microelectronics H4102, (125Khz, 26bit) s ID držitele, dobou platnosti, jsou barevně rozlišeny, zda se jedná o zaměstnance, studenta případně externího pracovníka. Návštěvní karty nebo identifikační karty pro servisní firmy jsou k dispozici v recepci objektu. Uvolnění elektromagnetických otevíračů je umožněno po verifikaci identifikačního čísla karty s uloženými daty v hlavní řídicí jednotce a systémového serveru. Elektromagnetické otevírače na únikových cestách jsou v případě signálu POŽÁR prostřednictvím NC výstupů systému EPS uvolněny a je umožněna bezpečná evakuace osob.

5.6.3 Stávající dohledový systém

Pro monitorování a záznam aktivity ve snímaných scénách, průchod osob v běžném provozu, vně i uvnitř modelového objektu, je instalován systém CCTV. Jedná se o triplexní systém, který je schopen v jednom okamžiku zobrazovat scény z vybraných kamer v reálném čase, vyhledat a přehrát záznam a provádět záznam. Je tvořen přehledovými kamerami ve venkovním vyhřívaném krytu pro venkovní scény a ve vnitřním boxovém provedení pro vnitřní záběry. Osvětlení venkovní snímané scény je zdroji z veřejného osvětlení, vnitřní přisvětlení jejich zbytkovým světlem. Napájení kamer je 230V/50Hz. Výstupní signál ze všech kamer je vyveden na monitorech sledovacího systému v prostoru recepce v 1.np., zde je na klientské stanici instalován volně dostupný klientský software SW klient Miles-

tone XPROTEC Smart pro práci s živým obrazem i s obrazem ze záznamu.

Rozmístění stávajících kamer:

- hlavní vstup – příchodová,
- zadní vstup – příchodová,
- ústav tělovýchovy a sportu – příchodová,
- manipulační prostor rampa – přehledová,
- služební parkoviště – přehledová,
- hřiště – přehledová,
- tělocvična – přehledová,
- posilovna – přehledová,
- vstup U56, kopírka hala – přehledová.

5.6.4 Stávající EPS

V modelovém objektu, jsou z hlediska požární bezpečnosti budovy, instalovány systémy elektrické požární signalizace EPS. Systém EPS LOOP500 a IQ8 M ESSER. Jejich instalace má především preventivní charakter, nezamezí vzniku požáru, ale včas jej detekuje. Hlásiče systému EPS jsou rozmístěny ve vytipovaných místnostech dle charakteru a důležitosti, podle svých vlastností odpovídají charakteristice daného prostředí (rychle hořící látky, látky, které uvolňují značné množství kouře, agresivní nebo jedovaté chemikálie). Poplachová informace která vzniká na výstupu jednotlivých hlásičů je přenesena kruhovým vedením do ústředny EPS. Ústředny EPS zajistí zpracování a předání informace ostraze objektu. Celý systém je SW rozdělen do skupin hlásičů, které jsou v souladu se schváleným požárně bezpečnostním řešením stavby. Nastavení systému, aktivuje výstupní obvody, které zajistí uvolnění únikových východů (odpojením napájení k elektromagnetickým dveřním otvíračům) v případě evakuace osob. Oba systémy jsou schopny pracovat v režimech NOC a DEN. V režimu DEN umožňují obsluhu systému v časovém intervalu T1 na ústředně systému přijmout a potvrdit informaci o místě vzniku požáru a spustí časový interval T2 ke kontrole místa vzniku požáru. Po ukončení T2 jsou automaticky aktivovány výstupy systému EPS. Automatické spuštění naprogramovaných výstupů proběhne také v případě aktivace manuálního hlásiče požáru, v případě že ústředna systému je provozována v režimu NOC tzn. bez obsluhy.

5.6.5 Stávající MZS

Základním prostředkem technického zabezpečení jsou prvky mechanických zábranných systémů, které zamezují vniknutí do chráněných prostor v objektu. Modelový objekt je z hlediska MZS vybaven standardními mechanickými uzamykacími systémy BT2, vybrané prostory BT3 dle ČSN EN 1627 a ČSN EN 1303. Klíčové hospodářství je řešeno prostřednictvím částečného systému generálního klíče, které se vztahuje na technické a technologické místnosti. Ostatní kancelářské a pobytové místnosti nejsou jeho součástí. Zapůjčení klíčů od společných prostor je možné v prostoru recepcce.

5.7 Návrh řešení

V rámci rekonstrukce stávajících bezpečnostních technologií je, dle požadavku na zvýšení ochrany osob a majetku v návrhu, uvažováno s kompletní plášťovou ochranou. Všechny otvíravé plochy, jako jsou okna a dveře přístupné z venku a nacházející se na vnějším plášti do úrovně 1.np, budou vybaveny magnetickými kontakty. V prostorech navazujících na plášťovou ochranu, na chodbách, v určených zájmových laboratořích, kancelářích apod. budou instalovány prostorové detektory s infračervenou a mikrovlnou složkou detekce (typ DUAL) k eliminaci vzniku falešných poplachů. Pro zvýšení bezpečnosti osob na pracovišti budou na vybraných pracovištích instalovány tísňové hlásiče pro signalizaci nebezpečí nebo pro přivolání pomoci prostřednictvím systému PZTS.

S přivoláním pomoci v předkládaném návrhu souvisí uvažované dorozumívací zařízení na bázi dveřních IP komunikátorů se symboly nouzového volání (SOS). Rozmístění komunikátorů je v hlavních komunikačních prostorech na vybraných místech. Komunikátory budou vzájemně propojeny prostřednictvím univerzální kabeláže (bezpečnostní síť) do místa trvalé obsluhy, která bude mít k dispozici systémový hands-free IP komunikátor. Dorozumívací systém bude svými výstupy propojen do systému PZTS.

Pro zamezení vstupu neoprávněných osob je v návrhu uvažováno zavést u všech vchodů do objektu bezkontaktní identifikaci osob na vstupu i výstupu. V prostoru hlavního vstupu je uvažováno směřovat pohyb přicházejících osob s oprávněním přes vstupní turnikety, osoby bez oprávnění navést k pracovišti ostrahy k zaevidování a vydání návštěvnické karty nebo zprostředkování odpovědného doprovodu. Aby nebyla snížena průchodná kapacita u hlavního vstupu, návrh uvažuje s instalací čtyř vstupních elektromechanických turniketů s propustností 40 osob za minutu (tj. 160 os./min. celkem), vstupně/výstupních terminálů bezkontaktních karet a mechanických zábran v prostoru vstupního foyer. Na výstupu bude

instalován automatický lapač návštěvnických karet s kapacitou 50 ks a možností rozšířit až na 300ks. Všechna vstupní a výstupní místa budou také zájmovými prostory pro dohledový systém. Před vybranými vstupy do zájmových prostor (speciální pracoviště, laboratoře, učebny s výpočetní technikou) je uvažováno rozmístit terminály čteček bezkontaktních karet s funkcí odblokování/zablokování podsystemu PZTS což vede k optimalizaci v obsluze bezpečnostního systému a současně přesné evidenci a identifikaci osob. Z pohledu požární bezpečnosti budou všechny systémové elektrické otvírače připojeny k rozpínacím kontaktům stávajícího systému EPS a na výstupní signál „požár“ budou uvolněny.

Pro zefektivnění výkonu fyzické ostrahy, (vizuální ověření příčiny poplachové situace), dokumentování dějů ve střežených a rizikových prostorech je uvažováno s instalací dohledového systému plně integrovaného do systému PZTS. Funkce instalovaných kamer se předpokládá jako přehledová v režimu rekognoskace (max. 50% snímané scény je sledovaný předmět)

V návrhu systému je pro zvýšení efektivity činnosti fyzické ostrahy dále uvažováno zavedení grafického nadstavbového systému, který datově komunikuje s připojenými bezpečnostními technologiemi a na grafickém rozhraní, monitoru, předkládá v reálném čase stavy jednotlivých detektorů. Rozmístění všech komponent bezpečnostních systémů je zřejmé z výkresové dokumentace v samostatné příloze

5.8 Popis technického řešení

Navrhované řešení resp., popis komponent, je členěno dle jednotlivých bezpečnostních technologií. Navrhovaný stav je zobrazen ve výkresové dokumentaci jednotlivých podlaží. Zde jsou také uvedeny podrobné tabulky místností pro možné SW členění navrhovaného řešení. Půdorysy jednotlivých podlaží s rozmístěním prvků bezpečnostních technologií jsou samostatnou přílohou této práce.

5.8.1 PZTS, SKV

Technologie

Na základě rozsahu objektu a s výhledem na možný požadavek budoucího rozšíření systému je uvažováno s integrovaným modulárním systémem PZTS a SKV pro střední a velké objekty. Jedná se o sběrníkový systém (RS 485) s možností redundantního provozu řídicích jednotek. Řídicí jednotky podporují on-line vzdálenou správu systému včetně aktualizací firmwaru. Z pohledu centrální správy se jedná o technologii klient – server na platformě

Microsoft SQL. Komunikace mezi systémovými prvky je šifrovaná dle AES-128. K systému je možno na 12-ti komunikačních linkách RS485 připojit až 360 modulů pro PZTS s 2872 vstupy, nebo 360 modulů pro SKV nebo jejich libovolné kombinace. Konfigurace SKV a PZTS probíhá prostřednictvím SW aplikace. Systém je možné členit do libovolného počtu podsystémů případně vytvářet skupiny a potom je ovládat prostřednictvím ovládacích panelů, integrovaného systému SKV, nebo SW klientské aplikace.

Jednotlivé moduly navrhovaného systému využívají komunikační sběrnice RS 485, která je společná pro všechny moduly systému PZTS, SKV.

Napájení

Napájení bude odpovídat požadavkům ČSN EN 50131-1 kapitola 9. Napájení systému bude ze zálohovaných zdrojů malého napětí typ A (základní zdroj+ dobíjený akumulátor) pro stupeň zabezpečení 2 doba zálohy 12hod. Během této doby musí být schopen poskytovat energii pro normální provoz včetně energie pro generování veškerých povinných indikací a hlášení vyplývající ze zpracování dvou samostatných signálů nebo zpráv [24].

Kabeláž

Kabelové rozvody budou realizovány podle platných předpisů, budou dodrženy zásady o označování kabelů, křížení, souběhu se silovými kabely. Hlavní rozvody budou uloženy ve stávajících kabelových trasách určených pro bezpečnostní technologie, ostatní kabeláž bude provedena v samostatných trubkách na příchytkách v podhledu, v technologických částech budou trasy přisazeny na stěnu. Pro komunikační sběrnice je uvažováno využít stíněných kabelů s kroucenými páry vodičů kategorie 5e.. Pro rozvody k detektorům instalovat kabely typu SYKFY 3x2x0,5.

Ovládání

Systém bude ovládán podle přidělených oprávnění ze systémového ovládacího panelu umístěného v recepci, nebo prostřednictvím terminálů systému SKV instalovaných u vstupu do zájmové oblasti. Systém bude SW nastaven dle požadovaných podsystémů. Výstup poplachové informace bude zobrazen v prostoru recepcie na samostatném systémovém ovládacím panelu a současně klientské aplikaci, která zajistí intuitivní ovládání rozsáhlého systému a navrhovaného integrovaného, monitorovacího a řídicího systému. Ze stejné klientské aplikace pak operátor bude provádět další činnosti (sledování stavu celého systému, evidenci návštěv, výdej návštěvních karet, vyhledávání v historii, správu uživatelů). Značnou přidanou hodnotou navrhovaného řešení je jednotná správa uživatelů pro systém PZTS

a SKV. Dále ve vazbě na dohledový systém umožní prostřednictvím instalované virtuální video matice zobrazit uživatele při průchodu definovaným vstupem. Ostraha může okamžitě identifikovat oprávněnost vstupující osoby.

5.8.2 Dohledový systém

Technologie

Ve vybraných zájmových prostorech budou instalovány přehledové Full HD IP kamery s integrovaným IR přísvitem, pro venkovní instalaci v krytu proti povětrnostním vlivům. Signál z těchto kamer bude prostřednictvím univerzální kabeláže přiveden na vstupy aktivních prvků v DR v technické místnosti recepce, a předán do digitální záznamové jednotky. Bude umístěna v technické místnosti v datovém rozvaděči bezpečnostních technologií. Nová jednotka bude propojena do systému prostřednictvím sítě LAN (bezpečnostní síť) a nakonfigurována do jednotného celku.

Systém bude provozován na platformě server – klient, kdy klientské pracoviště bude umístěno v prostoru recepce. Pracoviště bude vybaveno PC stanicí s výkonnou grafickou kartou pro připojení 4 LCD monitorů 24“, (zde bude umístěn také panel pro ovládání PZTS). V klidovém režimu budou na třech instalovaných monitorech zobrazeny všechny kamery v režimu 3x3 fullscreen. V případě poplachové události budou na poplachovém monitoru zobrazeny nejbližší 4 kamery v režimu „QUAD“. Záznam bude probíhat na vícenásobné diskové pole nezávislých disků (RAID5). Dle konfiguračního SW odpovídá instalovanému počtu kamer a nutné době záznamu diskový prostor o velikosti 5,5TB. Skutečný diskový prostor bude upraven dle zkušebního a následného provozu. Navrhované záznamové zařízení je možno rozšířit až na 48 TB v osmi slotech. Prostřednictvím SW nástroje bude permanentní záznam nastaven v kvalitě 3 fps a na 25fps v čase 5s od startu aktivity a 5s po ukončení aktivity ze systému PZTS. Další nastavení (uživatelský přístup, scény atp.) budou provedena dle požadavku uživatele.

Pro snížení rizika vzniku možných bezpečnostních incidentů (vandalismus, drobné krádeže, kapsářství), budou vnitřní kamery přisazeny na stěně na samostatných držácích, poloha nebude umožňovat snadnou manipulaci, poškození nebo zničení. Vnější kamery budou chráněny proti klimatickým a mechanickým vlivům pomocí vyhřívaných krytů. Jejich instalace bude provedena tak, aby bylo znemožněno jejich snadné úmyslné poškození nebo zcizení. Informace o pokusu zcizení kamery bude zanesena do systému PZTS. Současně bude jejich poloha umožňovat přístup pro údržbu, revizní, případně servisní práce.

Zřízení a provozování dohledového systému podléhá zákonu č. 101/2000 Sb. ve znění zákona č.183/2017 Sb. o ochraně osobních údajů. Dle znění tohoto zákona má správce dohledového systému ze zákona oznamovací / registrační povinnost vůči Úřadu pro ochranu osobních údajů. Dohledový systém je možné provozovat v případech:

- je-li to nezbytné pro ochranu práv a právem chráněných zájmů správce
- pokud je zpracování nezbytné pro dodržení právní povinnosti správce
- na základě souhlasu subjektu údajů

Poslední bod se se týká jen subjektů, kteří se ve sledovaném prostoru vyskytují pravidelně. Současně platí povinnost na viditelném místě označit sledovaný prostor informační tabulkou (např. prostor je monitorován) [40].

5.8.3 Dorozumívací systém

Technologie

Technologie dorozumívacího systému je založena na bázi IP jednotlačítkových dveřních komunikátorů s pictogramy (SOS) a v signálním oranžovém provedení. Dorozumívací systém je možné instalovat v hlavních komunikačních prostorech a ve vybraných prostorech. V místě trvalé obsluhy je navržen systémový hands-free komunikátor. Dle SW nastavení bude možné v případě zaneprázdněnosti obsluhy vyvolat další naprogramované funkce. Jakékoli zmáčknutí, včetně započítí, komunikace bude signalizováno v systému PZTS a současně na poplachovém monitoru zobrazeny nejbližší kamery dohledového systému.

Napájení

Pro napájení kamer a komunikátorů je uvažováno využití aktivních prvků s podporou PoE s dostatečně dimenzovaným výkonem. Napájení aktivních prvků bude z napájecí sítě 230V/50Hz, TN-C S se zálohou z UPS.

Kabeláž

Kabeláž pro kamerový a dorozumívací systém bude provedena jako topologie hvězda, bude respektovat mezinárodní standardy EIA/TIA 568B, ISO/IEC 11801, ČSN EN 50173 ed.3, ČSN EN 50174-2 ed.2, ČSN EN 50 288 -2-1 a 2. Pro modelový objekt je uvažována univerzální kabeláž pro dohledový systém s komponenty kategorie 5e, šířka pásma 100MHz.

5.8.4 Monitorovací a řídicí systém, grafická nástavba

Pro ještě efektivnější výkon fyzické ostrahy návrh uvažuje o nasazení integračního, monitorovacího a řídicího systému s grafickou nástavbou. Všechny bezpečnostní technologie (PZTS, SKV, EPS, CCTV) budou prostřednictvím TCP/IP protokolu posílat data na komunikační interface, ten je zpracuje a zapíše do SQL databáze. Díky obousměrné komunikaci bude mít operátor možnost přijímat informace a odesílat ovládací povely do konkrétních technologií. Pro snadnou lokalizaci monitorovaných oblastí jsou data ze všech bezpečnostních technologií navázána na vlastní grafické podklady. Obsluha tímto SW nástrojem získá srozumitelné a v jednotné podobě ovladatelné všechny připojené bezpečnostní technologie.

Přidanou hodnotou uvažovaného integračního systému je jednotné a intuitivní ovládání více technologií, obsluha může být školená na jeden systém s jedním pracovním prostředím.

5.9 Navrhovaná zařízení

Přehled základního navrhovaného zařízení je uveden v (Tab.14), rozmístění prvků a návrh vedení hlavních rozvodů je zřejmé z výkresové dokumentace v samostatné příloze.

Tab. 14 Seznam navrhovaného zařízení

PZTS - poplachový zabezpečovací a tísňový systém	
Zařízení	Popis
Ústředna PZTS	řídící jednotka PZTS,4 -12 sběrnice RS485, integrované SKV, neomezený počet podsystémů, neomezený počet uživatelů, neomezený počet přístupových karet, 2x LAN TCP/IP, RS-232, Stupeň 3. podle ČSN CLC/TS 50131-7
Linkový modul	přídavný sběrnice modul systému EZS pro připojení 8 dvojitě vyvážených zón, možnost připojení až osm volně programovatelných NO nebo NC bezpotenciálových výstupů, kompletní provedení včetně skříně s detekcí sabotáže, provedení min. pro stupeň zabezpečení 2
Ovládací panel	ovládací panel s alfanumerickou klávesnicí a LCD displejem 2x20 znaků pro ovládání systému EZS, se dvěma programovatelnými vstupy a výstupy s možností integrovat ACS
Přídavný zdroj +AKU	přídavný zálohovaný napájecí zdroj EZS 13,8V DC/ min. 5A+2A, včetně oceloplechové skříně s detekcí sabotáže, poruchy 230V, poruchy AKU, a prostorem pro akumulátor 40Ah. Provedení min. pro stupeň zabezpečení 2
Magnetické kontakty SET	magnetický kontakt pro zapuštěnou montáž na okna a dveře, 4 vodiče, délka kabelu 2m, pracovní mezera min 18mm, provedení pro stupeň zabezpečení 2
Propojovací krabice	propojovací krabice - 8 pájecích svorek + ochranný kryt, ochrana víčka proti proříznutí, instalace na omítku, certifikace min. pro stupeň zabezpečení 2
Prostorové detektory	infračervený pasivní + mikrovlnný prostorový detektor, dosah obou složek min. 15m při úhlu 85st., nastavení citlivosti, volba frekvence MW složky, stupeň zabezpečení 2
Nouzové tlačítko	tísňové tlač. bílé s ochr. odklápěcím krytem
Schránka pro klíč	Červená kovová skříňka s kládkem pro vyjmutí klíče
Systém Server	Server 1U rack, Intel Xeon E3-1220 v6, RAM 8GB DDR4 UDIMM, 1TB 7200 otáček SATA, max. 4x 3.5", SW RAID, iDRAC8 Basic, 2x GLAN, 250W, NBD on-site
PC Klientská stanice	CPU Intel® Core i7-5775C (3.3GHz, 6M, LGA1150, VGA) ASUS Z97-P 8GB DDR3-1600MHz Kingston HyperX Fury Blue, 2x4GB, HP NVIDIA Graphics PLUS NVS 315 1GB PCIe x16 1xDMS-59 (2x DVI), SD 2, 5" 180GB Intel® 535 series SATAIII 7mm, 19" IPC case do racku, 480mm hloubka, černý, Fortron FSP500-60GHN 80PLUS BRONZE, black, bulk 500W, MS Win Pro 8.1 Win64bit Czech 1pk OEM DVD,
LCD Monitor	LCD24" IPS 24/7, rozlišení 1920x1200, 16:9 podsvětlení typu IPS

SKV - systém kontroly vstupu	
Zařízení	Popis
Rídící jednotka	řídící jednotka SKV, integrována v PZTS
SW Server	Server advanced nadst. pro síť až 3 ústředěn
SW Klient	SW nástroj pro PC klientská stanice, ovládání, správa systému PZTS, SKV,
Dveřní jednotka	dveřní jednotka přístupového systému pro oboustranně zabezpečený vstup, jednotka umožňuje standardní funkce jako je monitorování stavu dveří, narušení průchodu, použití neplatné karty, monitorování stavu zámku, monitorování ochranného kontaktu řídicí jednotky, třída identifikace 2 nebo vyšší a přístupová třída B oboje dle souboru ČSN EN 60839-11-1, Napájení 11,5 až 13,8V společně pro desku elektroniky i zámku.
Terminál čtečky, čtečka	snímač čipových karet ve standardu MIFARE (13,56MHz).
Elektrický dveřní otvírač	signalizace stavu OTEVŘENÝCH nebo ZAVŘENÝCH dveří. trvalý provoz (denní režim) 11-13V DC, Odběr cívek 10-24V 130mA.
Dveřní zavírač	dveřní zavírač s hřebenovou technologií certifikován s lomeným ramínkem L190, Pro požárně odolné a kouřotěsné dveře do šířky 1100 mm a váhy 80 kg
Přídavný zdroj +AKU	přídavný zálohovaný napájecí zdroj EZS 13,8V DC/ min. 5A, včetně oceloplechové skříně s dedekcí sabotáže, poruchy 230V, poruchy AKU, a prostorem pro akumulátor 40Ah. Provedení min. pro stupeň zabezpečení 2
SOS komunikátor	bezpečnostní interkom pro nouzovou komunikace, automatické nastavení hlasitosti, reproduktor 10W, podsvícené tlačítko, podpora SIP protokolu, vzdálená správa, 2x NO/NC výstup na externí zařízení
Handsfree odpovídací komunikační jednotka	podpora HD aoudia, 7" dotykový displej, podpora zobrazení videa z externích kamer, informace o zmeškaném hovoru, vzdálená správa
Turniket	trnový turniket s trubkovou konstrukcí, mód oboustranného průchodu, výška 1,6m
Branka	nerozová křídlová branka se skleněnou výplní, Úhel otevření 0° - 270° pro každý směr
Lapač karet	Lapač karet EXI-R automatický sběr návštěvnických karet při východu.
Mechanická zábrana	nerozová konstrukce se skleněnou výplní, kotveno na chem kotvy

Televizní dohledový systém	
Zařízení	Popis
Server, záznamové zařízení	server s RAID systémem pro databázi - umožňuje nahrávat 64 IP kamer přes licenci CamConnect, komprese video MJPEG-H.264-H264CCTV-H265 HTTPS, 8 slotů RAID pro HDD max. 48TB, Rozhraní: DVI-D, DisplayPort, VGA, USB 3.0 2x, USB 2.0 Rozměr 482 x 133 x 543mm, 3U x 543mm pro 19" rack, napájení 110 - 240VAC/cca 240W, redundadní zdroje,
Kamera vnitřní	Systémová Full HD IP kamera řady G-Cam3 minidome krytu s IR přísvittem, Den/Noc s IR-C filtrem, 1/2.7" CMOS, objektiv 3 – 9mm/F1.2 vzdálené motorické ovládání zoomu a ostření, 16:9, Color 0,05Lx / BW 0,001Lx/32xSens-up, 1920x1080/30fps, ONVIF, AD, 100Mbit LAN, digitální vstup/výstup, napájení: PoE+ nebo 12VDC/24VAC max.20W, ,
Kamera venkovní	Systémová Full HD IP kamera ve venkovním kompaktním provedení typu Bullet s IR přísvittem, Den/Noc s IR-C filtrem, 1/2.8" CMOS 16:9, objektiv 3 – 9mm/F1.2, vzdálené motorické ovládání zoomu a ostření, Color 0,01Lx / BW 0,01Lx (50IRE/30pps), 1920x1080/50fps, digit. zoom x2 až x16, automatický BLC, WDR 96dB, Flip, Mirror, 2D/3D DNR, ONVIF, AD, 100Mbit LAN, digitální vstup/výstup, , dosvit LED max. 25m, napájení: PoE+ nebo 12-48VDC/24VAC max.cca 18W,
PC Klientská stanice	CPU Intel® Core i7-5775C (3.3GHz, 6M, LGA1150, VGA) - (výkonnější CPU než 4790 a hlavně výkonnější integrovaná GK – důležité pro výpočetní výkon při streamování videa) ASUS Z97-P 8GB DDR3-1600MHz Kingston HyperX Fury Blue, 2x4GB, HP NVIDIA Graphics PLUS NVS 315 1GB PCIe x16 1xDMS-59 (2x DVI), SD 2, 5" 180GB Intel® 535 series SATAIII 7mm, 19" IPC case do racku, 480mm hloubka, černý, Fortron FSP500-60GHN 80PLUS BRONZE, black, bulk 500W, MS Win Pro 8.1 Win64bit Czech 1pk OEM DVD,
LCD Monitor	LCD40" IPS 24/7, rozlišení 1920x1200, 16:9 podsvětlení typu IPS

Univerzální kabeláž	
Zařízení	Popis
Switch aktivní prvek	PoE switch 24/24+2 MNG, 24-portový switch PoE+ dle IEE802.af, 10/100Mbps, max proudový odběr 500W/19 Wport
Záložní UPS	APC Smart-UPS RT 1000VA RM online
Rack	19' rozvaděč stojanový 42U/800x800 skleněné dveře
Systémový podstavec	Podstavec 800x800 s filtrem 1x
Systémová police	Polička s perforací 1U/550mm, max.nosnost 40kg
Rozvod 230V	RAB-PD-X07-A1, 19' rozvodný panel, ČSN norma, 8 zásuvek,
Ventilační jednotka	Vent.j.spodní(horní)220V/60W 4 ventil. ,termostat RAL7035
Osvětlovací jednotka	19' osvětlovací jednotka 1U RAL7035

Monitorovací řídicí systém, grafická nastavba	
Zařízení	Popis
SW LAT	administrační nástroj správy do 200 ADVANCED Admin
SW LOW	pracoviště výkonného operátora (pro system ADVANC
SW LGLE	editor grafických projektů
SW LDE	data export Program pro export dat ze systému
SW LAOM	modul automatických činností Služba

Kompletní seznam navrhovaného zařízení včetně orientační cenové kalkulace je uveden v příloze P IV.

V (Tab. 15) je uvedena rekapitulace orientačních nákladů na komplexní rekonstrukci bezpečnostních technologií.

Tab. 15 Rekapitulace nákladů

Komplexní rekonstrukce bezpečnostních technologií - posílení zabezpečení		
PZTS - poplachový zabezpečovací a tísňový systém	753 019,00 Kč	265 761,00 Kč
SKV - systém kontroly vstupu	2 422 112,60 Kč	234 455,00 Kč
Televizní dohledový systém	838 094,00 Kč	73 495,00 Kč
Univerzální kabeláž	135 630,00 Kč	10 680,00 Kč
Monitorovací řídicí systém, grafická nastavba	81 700,00 Kč	70 360,00 Kč
CELKEM	4 230 555,60 Kč	654 751,00 Kč
DPH 21%	888 416,68 Kč	137 497,71 Kč
CELKEM s DPH	5 118 972,28 Kč	792 248,71 Kč
CELKEM s DPH		5 911 220,99 Kč

5.10 Konfigurace systému

V následující části budou uvedeny možnosti rozdělení celého systému na podsystémy. Navrhované zařízení umožňuje členit systém na libovolný počet podsystémů, vytvářet jejich skupiny a přidělovat je konkrétním uživatelům. Koncové SW nastavení systému je doporučeno dle požadavků koncového uživatele až při realizaci návrhu. V následující tabulce (Tab. 16) je uveden příklad členění a návrh možného postupu při zpracování podkladů pro SW nastavení systému.

Tab. 16 Princip členění systému

Označení	Skupiny podsystémů dle charakteristických prostor	Označení	Název podsystému	vstup/smyčka		
A/a	Hlavní vstup	Z/v	Hlavní vstup	Dveře MK		
				Prostor foyer		
B/b	Zadní vstupy	Z/v	Zadní vstup	Dveře MK		
				Prostor		
				Dveře MK		
		Z/v	Rampa	Prostor chodba		
				Z/v	Trafostanice	Dveře MK
C/c	Chodby	Z/v	Chodba 1.np	Okna MK		
				Prostor		
				Okna MK		
		Z/v	Chodba 2.np	Prostor		
				Z/v	Chodba 3.np	Okna MK
		Z/v		Prostor		
				Z/v	Učebny 1.np	Dveře MK
D/d	Učebny	Z/v	Učebny2.np	Prostor		
				Z/v	Učebny 3.np	Dveře MK
				Z/v		Prostor
E/e	Kanceláře 2.np	Z/v	Kancelář A210	Dveře MK		
				Prostor		
				Z/v	Kanceláře A211	Dveře MK
		Z/v	Kanceláře A212	Prostor		
				Z/v	Kanceláře A315	Dveře MK
F/f	Kanceláře 3.np	Z/v	Kanceláře A316	Prostor		
				Z/v	Kanceláře A317	Dveře MK
				Z/v		Prostor
G/g	Kanceláře 8.np	Z/v	Kanceláře A810	Dveře MK		
H/h	Technické m.	Z/v	Server	Prostor		
				Z/v	Ústředna SLP	Dveře MK
				Z/v	Strojovna VZT	Prostor

5.11 Uvedení do provozu, servis a údržba

Po ukončení realizace, která bude probíhat dodavatelským způsobem podle schválené dokumentace k provedení stavby, bude následovat kontrola kompletnosti dodávky, budou provedeny nutné funkční zkoušky a provedena výchozí revize z pohledu elektrické bezpečnosti zařízení. Případné odchylky od realizační dokumentace budou odsouhlaseny a zapracovány do dokumentace skutečné provedení. Následuje etapa zkušebního provozu, během kterého jsou zaznamenány a ihned odstraněny zjištěné nedostatky. Pak bude systém

uveden do trvalého provozu.

V průběhu běžného provozu je pracovník zodpovědný za provoz systému povinen zřídit a vést provozní knihu každého systému. Zde se zaznamenávají poplachové, poruchové stavy, zápisy o provedených kontrolách, oznámení poruchových stavů servisní organizaci, termín a způsob odstranění.

5.12 Dílčí závěr

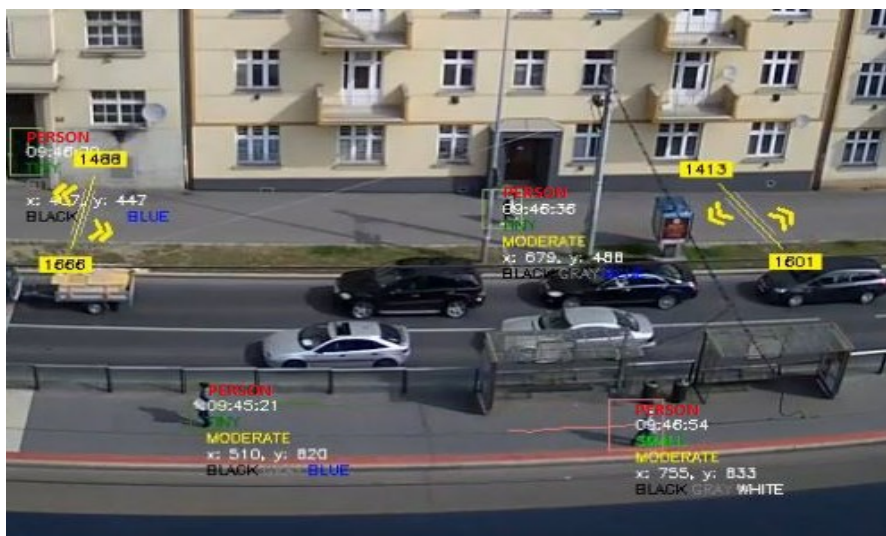
Na základě bezpečnostního posouzení, rozsahu potřebného zabezpečení, požadavku dle zadání jsem zvolil integrovaný modulární zabezpečovací systém pro střední a velké aplikace. Celkové řešení vede ke zvýšení bezpečnosti studentů i zaměstnanců při pracovní činnosti v objektu vysoké školy, vede k získání přehledu o pohybu osob v objektu a to především při vzniku mimořádné situace, kdy umožní rychlé, účinné a poskytnutí pomoci.

Zamezením vstupu neoprávněných osob se snižuje riziko možného vnášení/vynášení předmětů, nebo vstupu nežádoucích osob. Navrhované technické řešení, ve vztahu k fyzické ostraze, přispívá k efektivnímu vyhodnocení vzniklých mimořádných situací svým jednotným grafickým prostředím a tím umožní včas a účinně pomoci nebo pomoc přivolat.

6 TRENDY V ZABEZPEČENÍ OBJEKTŮ VYSOKÝCH ŠKOL PROSTŘEDNICTVÍM POKROČILÝCH TECHNICKÝCH PROSTŘEDKŮ

Současné využití bezpečnostních systémů díky narůstající kriminalitě neustále roste. Je jisté, že bezpečnostní systémy jsou dnes již samozřejmou součástí většiny objektů, přesto se neustále objevují pokusy o jejich překonání. Tento fakt posouvá vývoj a výrobu bezpečnostních technologií k využívání moderních technologických postupů s cílem dosáhnout na technicky dokonalá zařízení, spolehlivá při detekci i provozu a s intuitivním, „smart“ ovládáním. S prohlubujícím se trendem automatizace, robotizace a využívání umělé inteligence, výrobci přicházejí na trh s novými zařízeními, která toho využívají a jsou schopna se adaptovat v daném prostředí. Největší vývoj zaznamenává zřejmě oblast dohledových systémů, kdy díky vývoji v oboru IT a vývoji v SW nástrojů se snižuje časová náročnost a přitom zvyšuje přesnost a včasnost vyhodnocení při práci s těmito zařízeními. Obecně je cílem vývoje nových zařízení zvýšení jejich odolnosti proti různým typům napadení, zvýšení schopnosti detekce či zvýšení rychlosti přenosu obrazu, nebo informace o narušení apod.

Nasazení umělé inteligence v bezpečnostních zařízeních lze demonstrovat v oblasti dohledových systémů na sofistikovaném SW nástroji „CertiConVis“, který je ve světovém měřítku, považován za špičku. Jedná se o nástroj, který je využíván k detekci podezřelého chování subjektu v monitorovaném prostoru. Základem je detekce a rozpoznání objektu v monitorovaném prostoru (Obr.1).



Obr. 1 Rozpoznání objektů [41]

Objekt je pomocí metod umělé inteligence zařazen do jedné z několika tříd. Nástroj v reálném čase odhadne velikost, rychlost, barvu, polohu objektu jako základní a nutné informace k vyhodnocení dalších událostí (odhad vlastností objektu, maskování obrazového šumu apod.). Na rozdíl od běžně dostupných produktů tento nástroj pomocí neuronové sítě rozlišuje typy subjektů (vozidlo, člověk, zvíře apod.). Jeho chování je následně vyhodnocováno speciálními funkcemi, které zaznamenávají parametry trajektorie pohybu, trvání prostojů a vyhledávají v nich podezřelé vzory chování (náhlá změna rychlosti, náhlá změna směru, délka prostojů). Díky spojení několika analytických nástrojů pro forenzní a „realtime“ analýzu je schopen sloučit několikahodinové video v komprimovaném videu a zobrazit jej simultánně v několika minutách a s automatickou analýzou vyhodnotit a reagovat na podezřelé chování bez nutnosti uchování kamerových záznamů [42]. To má velký význam z pohledu nových požadavků na ochranu osobních údajů (nastupující GDPR) [43]. Události je možné flexibilně např. na základě typu nebo vlastností filtrovat a zobrazit jen např. červená vozidla v jednom směru.

Využití tohoto nástroje je široké, veřejné prostory, nákupní centra letiště, nádraží, školy, parkoviště.



Obr. 2 Sjednocení událostí v obraze [42]

Z bezpečnostního pohledu detekce nezvyklého chování osob slouží jako prevence, upozornění na budoucí incident v monitorované scéně. Detekce podezřelého chování vozidel (vozidlo ve špatném směru, vjezd vozidla do zakázané zóny, zakázaná změna směru, přetíženost dopravy) slouží k zamezení nebezpečných situací v dopravním provozu [42].

Dalším příkladem nasazení umělé inteligence a určení směru vývoje v bezpečnostních technologiích resp., opět v prostředí pokročilé video analýzy, je extrémně efektivní a rychlý nástroj rozpoznání zbraně ve videu v reálném čase a s velmi nízkou chybovostí. Aplikace vyvíjeného systému je velmi jednoduchá, může být nasazena i na starší systémy. To může vést k zajištění vyšší bezpečnosti ve většině instalací ve všech sférách hospodářství včetně objektů vysokých škol.

V současnosti může tuto nebezpečnou situaci se zbraní v obraze rozpoznat a nahlásit pouze člověk. Vyvíjený systém je díky umělé inteligenci při detekci velice efektivní, neúnavný a na rozdíl od množství lidí potřebných ke sledování třeba i tisíců živých streamů i ze sociálních sítí velmi levný. Systém opět využívá techniky konvolučních neuronových sítí (CNN – Convolutional Neural Networks) byl testován také na obrazech nízké kvality (YouTube), to z důvodu využití u starších dohledových systémů. Uspokojivý výsledek vedl k definici nové metriky Alarm Activation Per Interval (AApI), která hodnotí výkon automatického detekčního systému ve videu. Je zřejmé, že pokud se někde objeví zbraň, vzniká velmi nebezpečná a náhlá situace, při které může dojít k tragické události, jak se již také mnohokrát stalo. Popisovaný systém je schopen reagovat již ve fázi přípravy či kontroly zbraně před budovou nebo na chodbě a předat včasnou poplachovou informaci [41].



Obr. 3 Detekce zbraně [41]

Uvedené nástroje souvisí s efektivitou dohledových systémů. V rozsáhlých instalacích je pořizováno nemalé množství hodin záznamu, jsou budovány masivní datové rozvody a finančně nákladná datová úložiště. Je rozmisťováno nemalé množství kamer, které jsou,

ale svedeny na centrální pracoviště s operátory, kteří mají jen minimální šanci zaznamenat v reálném čase potenciální nebezpečnou situaci a tím pádem v předstihu a včas reagovat.

6.1.1 Dílčí závěr

Pro zabezpečení objektů vysokých škol nejsou vyvíjeny speciální prvky bezpečnostních technologií, jsou využívána běžně dostupná zařízení, přičemž je nutné využít jejich vlastností a vhodně je kombinovat. Technické prostředky bezpečnostních technologií se stávají stále sofistikovanějšími nástroji, vedoucími k vyšší bezpečnosti a lze je využít ve všech sférách hospodářství.

V současnosti lze odhadnout trend vývoje jen těžko, přesto je zavedena výroba bezpečnostních zařízení a nástrojů prostřednictvím poloautomatických, automatických, robotických výrobních linek. Přesnost přispívá ke spolehlivosti. Předpokládá se vývoj HW a SW nástrojů pro uživatelsky přívětivé ovládání „smart“ zařízení. S tím také souvisí zajištění vyšší bezpečnosti uložených nutně získaných dat zejména v případě cloudového řešení HW. Do analytických SW nástrojů jsou vkládány prvky umělé inteligence, řeší se požadavky na minimální chybovost vedoucí k zvýšení jejich spolehlivosti.

Uvedené nástroje pro zdokonalení dohledových systémů, ale také souvisí s částečnou ztrátou anonymity osob, která je vnímána jako nedotknutelná. O ztrátě anonymity hovoříme v případech, kdy jsou shromažďována naše osobní data v dohledových systémech, a to z hlediska jejich zneužití jinou osobou. To platí jen do doby, než se něco stane. Umělá inteligence však nepotřebuje naše data zneužívat. Naopak uvedené nástroje dokáží zabránit úrazům, nehodám, úmrtím lidí, nebo škodám na majetku. Současně platí, že vhodně umístěná kamera působí preventivně, odradí potenciální pachatele, zajistí nepopiratelné důkazy. Pokud hovoříme o zneužívání osobních dat, musíme také řešit, jakým způsobem je ochránit proti zneužití („kdo bude hlídat hlídače“).

ZÁVĚR

Bezpečnostní systémy jsou nedílnou součástí, standardem ve vybavenosti většiny objektů v soukromém i veřejném sektoru. Jsou instalovány k podpoře ochrany majetku a osob. Přispívají k včasnému a efektivnímu vyřešení bezpečnostní situace.

Cílem práce bylo vytvořit návrh komplexního zabezpečení modelového objektu vysoké školy, který je založen na reálném objektu a může být využit jako podpůrný materiál při návrhu technického řešení pro reálné objekty vysokých škol.

V teoretické části jsou předloženy základní legislativní a technické předpisy, které se vztahují k problematice vysokých škol, technických předpisů ve vztahu k bezpečnému provozu budov a poznatky získané z odborné literatury nebo ostatních zdrojů.

Praktická část se je v úvodu zaměřena na analýzu vybraných objektů vysokých škol s rozdílným oborovým, studijním zaměřením a rozdílným provozním rozsahem. Cílem bylo analyzovat stávající stav zabezpečení z pohledu ochrany osob a majetku, provozu budovy, zavedených režimových opatření a určit základní typy prostor a jejich specifické provozní vlastnosti. V další části bylo zpracováno bezpečnostní posouzení modelového objektu z pohledu možných rizik a možných ostatních vlivů působících na objekt. Na tomto základě byl proveden návrh komplexního zabezpečení pro možnou rekonstrukci stávajících bezpečnostních systémů.

V posledním bodě, jsou předloženy nastupující trendy v oblasti zabezpečení objektů, zejména v oblasti dohledových systémů. Díky SW nástrojům, které využívají umělé inteligence, se dostávají do popředí zájmu i z hlediska nastupujícího GDPR.

Přidanou hodnotu práce je její podpůrná funkce při zřizování návrhu komplexního efektivního zabezpečení pro rozlehlý univerzitní kampus, samostatnou budovu univerzity nebo menší objekt školy. Efektivní bezpečnost přitom začíná společným vývojem detailní bezpečnostní koncepce, v níž je bráno v podvědomí uspořádání budov, chování studentů, zaměstnanců, jasné stanovení odpovědnosti a pravidel pro externí pracovníky a vytyčení technických požadavků na bezpečnostní systémy.

CONCLUSION

Security systems are an integral part, a standard in the facilities of most premises in the both private and public sector. They are installed to help support the protection of property and persons. They contribute to the timely and effective resolution of the security situation.

The aim of the thesis was to create a proposal for a comprehensive security model of university premises, which is based on a real area and can be used as supporting material for the proposal of a technical solution for real university premises.

In the theoretical part are presented basic legislative and technical regulations relating to the issues of universities, technical regulations in relation to the safe operation of buildings and knowledge gained from professional literature and other sources.

The practical part is in the introduction focused on the analysis of selected university premises with different fields of study, study orientation and different operational scopes. The aim was to analyse the current state of security from the point of view of protection of persons and property, operation of the building, established regime measures and to determine the basic types of area and their specific operating characteristics. In the next part, a safety assessment of the modelled premises was developed from the point of view of potential risks and other potential influences affecting the premises. On this basis, a comprehensive security proposal was designed for possible reconstruction of existing security systems.

In the final point, emerging trends in object security are presented, especially in the field of surveillance systems. Thanks to SW tools that use artificial intelligence, GDPR also comes to the forefront of interest.

The added value of the work is its supporting function when establishing a comprehensive effective security proposal for a large university campus, a separate university building or a smaller school building. Effective security starts with the development of a detailed security concept that takes into account building arrangements, student and employee behaviour, clear establishment of responsibility and rules for external staff, and setting technical requirements for security systems.

SEZNAM POUŽITÉ LITERATURY

- [1] ČESKÁ REPUBLIKA. Zákon č. 89/2012 Sb. občanský zákoník. In: □*Sbírka zákonů ČR*. Praha, 2012, částka 33, číslo 89, s. 1026-1365.
- [2] ČESKÁ REPUBLIKA. Zákon č. 262/2006 Sb. Zákoník práce. In: □*Sbírka zákonů ČR*. Praha, 2006, částka 84, číslo 262, s. 3146-3272.
- [3] ČESKÁ REPUBLIKA. Zákon č. 219/2000 Sb. o majetku ČR a jejím vystupování v právních vztazích. In: □*Sbírka zákonů ČR*. Praha, 2000, částka 33, číslo 219, s. 3129-3146.
- [4] ČESKÁ REPUBLIKA. Zákon č. 218/2000 Sb. o rozpočtových pravidlech. In: □*Sbírka zákonů ČR*. Praha, 2000, částka 65, číslo 218, s. 3104-3128.
- [5] ČESKÁ REPUBLIKA. Zákon č. 563/1991 Sb. o účetnictví. In: □*Sbírka zákonů ČR*. Praha, 1991, částka 39, číslo 563, s. 5388-5419.
- [6] ČESKÁ REPUBLIKA. Zákon č. 111/1998 Sb. o vysokých školách. In: □*Sbírka zákonů ČR*. Praha, 1998, částka 39, číslo 111, s. 5388-5419.
- [7] ČESKÁ REPUBLIKA. Vyhláška č. 504/2002 Sb. kterou se provádějí některá ustanovení zákona č. 563/1991 Sb. In: □*Sbírka zákonů ČR*. Praha, 2012, částka 174, číslo 504, s. 9809-9844.
- [8] ČESKÁ REPUBLIKA. Zákon č. 106/1999 Sb. o svobodném přístupu k informacím. In: □*Sbírka zákonů ČR*. Praha, 1999, částka 39, číslo 106, s. 2578-2582.
- [9] ČESKÁ REPUBLIKA. Zákon č. 309/2006 Sb. Další požadavky bezpečnosti a ochrany zdraví při práci v pracovně právních vztazích. In: □*Sbírka zákonů ČR*. Praha, 2006, částka 96, číslo 309, s. 3789-3797.
- [10] ČESKÁ REPUBLIKA. Zákon č. 183/2006 Sb. o územním plánování a stavebním řádu. In: □*Sbírka zákonů ČR*. Praha, 2006, částka 63, číslo 183, s. 2226-2290.
- [11] ČESKÁ REPUBLIKA. Zákon č. 133/1985 Sb. o požární ochraně. In: □*Sbírka zákonů ČR*. Praha, 1985, částka 34, číslo 133, s. 674-691.

- [12] ČESKÁ REPUBLIKA. Vyhláška č. 246/2001 Sb. o stanovení požární bezpečnosti a výkonu státního požárního dozoru. In: □*Sbírka zákonů ČR*. Praha, 2001, částka 95, číslo 246, s. 5446-5489.
- [13] ČESKÁ REPUBLIKA. Vyhláška č. 23/2008 Sb. o technických podmínkách požární ochrany. In: □*Sbírka zákonů ČR*. Praha: Ministerstvo vnitra, 2008, částka 10, číslo 23, s. 478-506.
- [14] ČESKÁ REPUBLIKA. Legislativní pravidla vlády. In: *Legislativní pravidla vlády ČR*. Praha: Legislativní rada státu, 2010, s. 69. Dostupné také z: <https://www.vlada.cz/cz/ppov/lrv/dokumenty/legislativni-pravidla-vlady-91209/>
- [15] ŠÍN, Zbyněk. *Tvorba práva: pravidla, metodika, technika*. Vyd. 2. V Praze: C.H. Beck, 2009. Beckovy příručky pro právní praxi. ISBN 978-80-7400-162-8.
- [16] GERLOCH, Aleš. *Teorie práva*. 6., aktualiz. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2013. ISBN 978-80-7380-454-1.
- [17] HENDRYCH, Dušan. *Právní slovník*. 2. rozš. vyd. Praha: C.H. Beck, 2003. Beckovy odborné slovníky. ISBN 80-7179-740-5.
- [18] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management*. 1. vydání. Zlín: Radim Bačuvčík - VeRBuM, 2011-2015. ISBN 978-80-87500-67-5.
- [19] VALOUCH, Jan. *Projektování bezpečnostních systémů*. První. Zlín: Univerzita Tomáše Bati ve Zlíně, 2012, 152 s. ISBN 978-80-7454-230-5.
- [20] ČSN EN 73 4400. *Prevence kriminality - řízení bezpečnosti při plánování, realizaci a užívání škol a školských zařízení*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2016, 44 s.
- [21] SLADKÝ, Libor. *Bezpečnost školských zařízení, ČSN 73 4400 - aplikace a metodika*. 2. zkácená verze. Praha: Ministerstvo vnitra ČR, 2017.
- [22] URBAN, Miroslav. *Moderní evropský standard zabezpečení*. Sborníky technické harmonizace ÚNMZ. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.
- [23] ČSN EN 14383-1. *Prevence kriminality - Plánování městské výstavby a navrhování*

- budov*. Praha: Český normalizační institut, 2007, 16 s.
- [24] ČSN CLC/TS 50131-7. *Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 7*. Praha: Český normalizační institut, 2011, 44 s.
- [25] TNI 33 4591-1. *Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 1: Návrh systému PZTS - Komentář k ČSN CLC/TS 50131-7*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2012, 16 s.
- [26] ČSN 76 1702. *Poskytovatelé bezpečnostních služeb - Fyzická ostraha - Požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014, 20 s.
- [27] Národní ústav pro vzdělávání. *Národní soustava kvalifikací* [online]. Praha: NÚV a TREXIMA spol. s r.o., 2015 [cit. 2018-02-21]. Dostupné z: <https://www.narodnikvalifikace.cz/kvalifikace-315-Strazny/revize-1386/kvalifikacni-standard>
- [28] BRABEC, František. *Ochrana bezpečnosti podniku*. Vyd. 1. Praha: Eurounion, 1996. ISBN 80-858-5829-0.
- [29] KINDL, Jiří. *Projektování bezpečnostních systémů*. Vyd. 2. Zlín: Univerzita Tomáše Bati, 2007. ISBN 978-80-7318-554-1.
- [30] TZB info. *TZB info* [online]. b.r. [cit. 2018-02-21]. Dostupné z: <https://www.tzb-info.cz/kamerove-systemy>
- [31] PAULSSON, Johan. Jak vypadají moderní dohledové systémy ? (2). *COMPUTERWORLD: SecurityWorld* [online]. b.r. [cit. 2018-02-21]. Dostupné z: <https://computerworld.cz/securityworld/dohledove-systemy-v-roce-2015-2-52211>
- [32] ČSN EN 50134-1. *Poplachové systémy - Systémy přivolání pomoci Část 1: Systémové požadavky*. Praha: Český normalizační institut, 2003, 12 s.
- [33] BEBČÁK, Petr. *Požárně bezpečnostní zařízení*. 2. rozšířené vydání. V Ostravě: Sdružení požárního a bezpečnostního inženýrství, 2004. Spektrum (Sdružení požárního a bezpečnostního inženýrství). ISBN isbn80-86634-34-5.
- [34] ISO 7240-16. *Fire detection and alarm systems - Part 16: Sound system control and indicating equipment*. Geneva: International organization for standardization, 2007.

- [35] ŠKRABAL, Josef a Radek HAVEL. *Počet obyvatel v obcích k 1.1.2017* [online]. Praha: Český statistický úřad, 2017, , 120 [cit. 2018-02-21]. Dostupné z: <https://www.czso.cz/documents/10180/45964084/13007217.pdf/16152f21-3984-4ada-8599-be35c0e31ad6?version=1.1>
- [36] HUDCOVÁ, Pavla a Miroslav MAŠEK. *Masarykova univerzita*. Brno: Masarykova univerzita, 2010.
- [37] Masarykova univerzita. *Univerzitní kampus, MAPA* [online]. 2018 [cit. 2018-02-15]. Dostupné z: <https://www.muni.cz/mapa/lekarska-fakulta>
- [38] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013. Expert (Grada). ISBN 978-80-247-4644-9.
- [39] ČSN EN 60839 -11-1. *Poplachové a elektronické bezpečnostní systémy- Část 11-1: Elektronické systémy kontroly vstupu- Požadavky na systém a komponenty*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014, 56 s.
- [40] *Provozování kamerových systémů*. Praha: Úřad pro ochranu osobních údajů, 2012. ISBN 978-80-210-6017-3.
- [41] OLMOS, Roberto, Siham TABIK a Francisco HERRERA. *Automatic Handgun Detection Alarm in Videos Using Deep Learning*. Department of Computer Science and Artificial Intelligence, 2017. University of Granada.
- [42] *CertiConVis* [online]. Praha, 2016 [cit. 2018-04-19]. Dostupné z: <http://www.certiconvis.cz>
- [43] IDNES.cz/Zprávy. *Češi na špicce oboru umělé inteligence* [online]. Praha: MAFRA,a.s., 2018 [cit. 2018-04-20]. Dostupné z: https://sdeleni.idnes.cz/cesi-na-spicce-oboru-umele-inteligence-v-oblasti-bezpecnosti-pr7-/zpr_sdeleni.aspx?c=A180326_130102_zpr_sdeleni_rest

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ARC	Alarm Reciving Centre
I&HAS	Intrusion and Hold-up Alarm System
CCTV	Surreillance systems for use in security applications
PTZ	Rotace kamery + zoom (přiblížení)
ACCESS	Access kontrol systems for use in security applications
SAS	Social alarm systems
PZTS	Poplachový zabezpečovací a tísňový systém
EKV	Elektronická kontrola vstupu
RFID	Radio Frequency Identification/ Identifikace na rádiové frekvenci
DPPC	Poplachové přijímací dohledové centrum
EPS	Elektrická požární signalizace
LCD	Liquid - crystal display/ zobrazovací technologie
ICT	Informační a komunikační technologie
PC	Počítač
HW	Hardware
SW	Software
LAN	Lokální síť počítačů (Local Area Network)
SQL	Standardizovaný strukturovaný dotazovací jazyk (Structured Query Language)
TCP/IP	Primární přenosový protokol/ protokol síťové vrstvy (Transmission Control Protocol/Internet Protocol)
PIN	Osobní identifikační číslo (Personal Identification Number)
BT	Bezpečnostní třída
MŠMT ČR	Ministerstvo školství, mládeže a tělovýchovy České republiky

SEZNAM OBRÁZKŮ

Obr. 1	Rozpoznání objektů [41]	84
Obr. 2	Sjednocení událostí v obraze [42]	85
Obr. 3	Detekce zbraně [41]	86

SEZNAM TABULEK

Tab. 1	Typické prostory - univerzitní kampus	40
Tab. 2	Typické prostory - univerzita	44
Tab. 3	Typické prostory - soukromá vysoká škola.....	47
Tab. 4	Charakteristika objektů	49
Tab. 5	Bodové ohodnocení důležitosti aktiv	55
Tab. 6	Bodové hodnocení zranitelnosti aktiv	56
Tab. 7	Klasifikace identifikovaných hrozeb.....	56
Tab. 8	Princip stanovení míry rizika a jeho přijatelnosti.....	57
Tab. 9	Přehled rizik	60
Tab. 10	Princip stanovení působení vlivu a jeho přijatelnosti.....	62
Tab. 11	Vyhodnocení působení vnitřních vlivů	63
Tab. 12	Vyhodnocení vnějších vlivů	64
Tab. 13	Třídy prostředí přehled	70
Tab. 14	Seznam navrhovaného zařízení	79
Tab. 15	Rekapitulace nákladů	81
Tab. 16	Princip členění systému.....	82

SEZNAM ROVNIC

Rovnice 1	Výsledná hodnota rizika.....	56
-----------	------------------------------	----

SEZNAM PŘÍLOH

- P I Seznam aktiv a hrozeb, Hodnocení aktiv, hrozeb, zranitelnosti, míry rizika
- P II Klasifikace aktiv dle zranitelnosti
- P III Stanovení míry rizika
- P IV Přehled navrhovaných zařízení, rekapitulace orientačních nákladů

PŘÍLOHA P I: SEZNAM AKTIV

1	Osoby
1.1	Zaměstnanci
1.2	Studenti
1.3	Externí zaměstnanci
1.4	Návštěvy
1.5	Zdravotně postižení, nemobilní občané
1.6	Rezerva 1
2	Informace
2.1	Průmyslové vlastnictví, dokumentace
2.2	Osobní údaje
2.3	Interní předpisy a nařízení
2.4	Rezerva 1
2.5	Rezerva 2
3	Okolí budovy
3.1	Vjezd na parkoviště, parkoviště
3.2	Perimetr
3.3	Plášť budovy
3.4	Rezerva 1
4	Budova
4.1	Hlavní vstup
4.2	Vedlejší vstup
4.3	Boční vstup
4.4	Nouzový východ
4.5	Zásobovací rampa
4.6	Odpadové hospodářství
4.7	Trafostanice
4.8	Samostatný vstup - Zpracování polymerů
4.9	Volné prostory, chodby
4.10	Pracovny
4.11	Kanceláře - pokladna, osobní údaje, Průmyslové vlastnictví, dokumentace
4.12	Technické provozní místnosti
4.13	Sklady
4.14	Archiv
4.15	Laboratoře
4.16	PC učebny
4.17	Přednáškové sály
4.18	Menza
4.19	Rezerva 1
5	Hmotný majetek
5.1	Hardware - výpočetní a komunikační technika
5.2	Technologie laboratoří, měřicí technika
5.3	Uložené věci
5.4	Technické bezpečnostní systémy
5.5	Komunikační prostředky
5.6	Ostatní hmotný majetek
5.7	Rezerva 1

SEZNAM HROZEB

1.	Technická selhání
1.1	Požár
1.2	Exploze
1.3	Destrukce budovy
1.4	Havárie vody
1.5	Havárie plynu
1.6	Havárie dodávky elektrické energie
1.7	Havárie topení
1.8	Havárie kanalizačního systému
1.9	Havárie spojovacích a datových sítí
1.10	Chybná správa (konfigurace systému sítí) IS/IT
1.11	Ztráta dat v IS/IT
1.12	Nedostatečná ochrana proti virům v IS/IT
1.13	Nechráněný přístup z vnějších sítí IS/IT
1.14	Selhání SW, HW, komunikací IS/IT
1.15	Nefunkčnost technických bezpečnostních opatření
1.16	Mechanická poškození
1.17	Rezerva 1
1.18	Rezerva 2
2.	Organizační nedostatky
2.1	Narušení procesů, činnosti
2.2	Nedostatečné materiálové kapacity/zdroje
2.3	Nedostatek pracovní síly
2.4	Chybná interpersonální komunikace
2.5	Rezerva 1
2.6	Rezerva 2
3.	Lidský faktor
3.1	Nedodržování režimových a organizačních opatření zaměstnanci
3.2	Nedodržování režimových a organizačních opatření studenti
3.3	Nedodržování režimových a organizačních opatření návštěvami
3.4	Nedostatečná kontrola vstupujících (vystupujících) osob
3.5	Chybné nakládání s osobními údaji
3.6	Neúmyslné poškození
3.7	Úraz
3.8	Rezerva 2
4.	Úmyslná škodlivá lidská činnost
4.1	Útok ozbrojené skupiny/jedince
4.2	Úmyslné poškození zaměstnanci
4.3	Úmyslné poškození studenti
4.4	Překonání bezpečnostních systémů
4.5	Vniknutí do objektu
4.6	Neoprávněný vstup
4.7	Vandalismus
4.8	Krádež
4.9	Rezerva 1
4.10	Rezerva 2
5.	Vyšší moc
5.1	Změna politického klimatu
5.2	Změna legislativy
5.3	Velké veřejné akce, demonstrace
5.4	Stávká

HODNOCENÍ AKTIV

Aktiva	
0	zanedbatelná
1	malá
2	nízká
3	střední
4	vyšší
5	velmi vysoká

HODNOCENÍ HROZEB

Hrozby	
0	žádná
1	zanedbatelná
2	nízká
3	střední
4	vyšší
5	velmi vysoká
6	jistá

HODNOCENÍ ZRANITELNOST

Zranitelnost	
0	žádná
1	nízká
2	střední
3	vyšší

HODNOCENÍ MÍRY RIZIKA

Kvantitativní hodnota míry rizika	Kvalitativní hodnota míry rizika	Barevné označení závažnosti rizika	Přijatelnost rizika
0 - 35	Malé riziko		Přijatelné
36 - 60	Střední riziko		Přechodné
61 - 90	Vysoké riziko		Nepřijatelné

PŘÍLOHA P IV PŘEHLED NAVRHOVANÝCH ZAŘÍZENÍ, REKAPITULACE ORIENTAČNÍCH NÁKLADŮ

Přehled navrhovaných zařízení

PZTS - poplachový zabezpečovací a tísňový systém							
Zařízení	Popis	Počet	MJ	Cena/MJ	Cena/dodávka	Montáž/MJ	Cena/montáž
Ústředna PZTS	řídící jednotka PZTS,4 -12 sběrnice RS485, integrované SKV, neomezený počet podsystémů, neomezený počet uživatelů, neomezený počet přístupových karet, 2x LAN TCP/IP, RS-232, Stupeň 3. podle ČSN CLC/TS 50131-7	1	ks	25 500,00 Kč	25 500,00 Kč	1 540,00 Kč	1 540,00 Kč
Linkový modul	přídavný sběrnice modul systému EZS pro připojení 8 dvojité vyvážených zón, možnost připojení až osm volně programovatelných NO nebo NC bezpotenciálových výstupů, kompletní provedení včetně skříně s detekcí sabotáže, provedení min. pro stupeň zabezpečení 2	57	ks	1 850,00 Kč	105 450,00 Kč	770,00 Kč	43 890,00 Kč
Ovládací panel	ovládací panel s alfanumerickou klávesnicí a LCD displejem 2x20 znaků pro ovládání systému EZS, se dvěma programovatelnými vstupy a výstupy s možností integrovat ACS	2	ks	3 420,00 Kč	6 840,00 Kč	385,00 Kč	770,00 Kč
Přídavný zdroj +AKU	přídavný zálohovaný napájecí zdroj EZS 13,8V DC/ min. 5A+2A, včetně oceloplechové skříně s detekcí sabotáže, poruchy 230V, poruchy AKU, a prostorem pro akumulátor 40Ah. Provedení min. pro stupeň zabezpečení 2	8	ks	5 500,00 Kč	44 000,00 Kč	690,00 Kč	5 520,00 Kč
Magnetické kontakty SET	magnetický kontakt pro zapuštěnou montáž na okna a dveře, 4 vodiče, délka kabelu 2m, pracovní mezera min 18mm, provedení pro stupeň zabezpečení 2	220	ks	327,00 Kč	71 940,00 Kč	256,00 Kč	56 320,00 Kč
Propojovací krabice	propojovací krabice - 8 pájecích svorek + ochranný kryt, ochrana víčka proti proříznutí, instalace na omítku, certifikace min. pro stupeň zabezpečení 2	138	ks	210,00 Kč	28 980,00 Kč	236,00 Kč	32 568,00 Kč
Prostorové detektory	infrachervený pasivní + mikrovlnný prostorový detektor, dosah obou složek min. 15m při úhlu 85st., nastavení citlivosti, volba frekvence MW složky, stupeň zabezpečení 2	104	ks	1 956,00 Kč	203 424,00 Kč	289,00 Kč	30 056,00 Kč
Nouzové tlačítko	tísňové tlač. bílé s ochr. odklápěcím krytem	65	ks	680,00 Kč	44 200,00 Kč	247,00 Kč	16 055,00 Kč
Schránka pro klíč	Červená kovová skříňka s kladívkem pro vyjmutí klíče	6	ks	240,00 Kč	1 440,00 Kč	247,00 Kč	1 482,00 Kč
Systém Server	Server 1U rack, Intel Xeon E3-1220 v6, RAM 8GB DDR4 UDIMM, 1TB 7200 otáček SATA, max. 4x 3,5", SW RAID, iDRAC8 Basic, 2x GLAN, 250W, NBD on-site	1	ks	72 600,00 Kč	72 600,00 Kč		0,00 Kč
PC Klientská stanice	CPU Intel® Core i7-5775C (3.3GHz, 6M, LGA1150, VGA) ASUS Z97-P 8GB DDR3-1600MHz Kingston HyperX Fury Blue, 2x4GB, HP NVIDIA Graphics PLUS NVS 315 1GB PCIe x16 1xDMS-59 (2x DVI), SD 2, 5" 180GB Intel® 535 series SATAIII 7mm, 19" IPC case do racku, 480mm hloubka, černý, Fortron FSP500-60GHN 80PLUS BRONZE, black, bulk 500W, MS Win Pro 8.1 Win64bit Czech 1pk OEM DVD,	1	ks	19 800,00 Kč	19 800,00 Kč		0,00 Kč
LCD Monitor	LCD24" IPS 24/7, rozlišení 1920x1200, 16:9 podsvětlení typu IPS	2	ks	8 700,00 Kč	17 400,00 Kč		0,00 Kč
SW Server	Server advanced nadst. pro síť až 3 ústředn	1	ks	18 600,00 Kč	18 600,00 Kč		0,00 Kč
SW Klient	SW nástroj pro PC klientská stanice, ovládání, správa systému PZTS, SKV,	1	ks	9 300,00 Kč	9 300,00 Kč		0,00 Kč
Oživení systému	Oživení systému najeden detektor	307	ks	0,00 Kč	0,00 Kč	180,00 Kč	55 260,00 Kč

PZTS - kabeláž							
PZTS	nízkofrekvenční kabel pro vnitřní instalace. Materiál vodičů Cu 6x0,5mm2, PVC izolace žil, elektrostatické stínění, PVC plášť, bílý nebo šedý	7500	m	6,44 Kč	48 300,00 Kč		0,00 Kč
PZTS	datový 4 párový stíněný FTP kabel cat.5E, izolace PVC -, určeno pro propojení systémové sběrnice bez nutnosti přenosu napájení	875	m	12,30 Kč	10 762,50 Kč		0,00 Kč
PZTS	napájecí kabel pro vnitřní použití, materiál vodičů Cu, 2x1,5mm2, izolace PVC	225	m	7,90 Kč	1 777,50 Kč		0,00 Kč
PZTS	napájecí kabel pro vnitřní použití, materiál vodičů Cu, 2x2,5mm2, izolace PVC	650	m	9,50 Kč	6 175,00 Kč		0,00 Kč
	Instalační materiál	1	kpl	16 530,00 Kč	16 530,00 Kč	22 300,00 Kč	22 300,00 Kč
CELKEM					753 019,00 Kč		265 761,00 Kč
DPH 21%					158 133,99 Kč		55 809,81 Kč
SKV - systém kontroly vstupu							
Zařízení	Popis	Počet	MJ	Cena/MJ	Cena/dodávka	Montáž/MJ	Cena/montáž
Řídicí jednotka	řídící jednotka SKV, integrována v PZTS	0	ks	25 500,00 Kč	0,00 Kč		0,00 Kč
SW Server	Server advanced nadst. pro síť až 3 ústředěn	0	ks	18 600,00 Kč	0,00 Kč		0,00 Kč
SW Klient	SW nástroj pro PC klientská stanice, ovládání, správa systému PZTS, SKV,	0	ks	18 600,00 Kč	0,00 Kč		0,00 Kč
Dveřní jednotka	dveřní jednotka přístupového systému pro oboustranně zabezpečený vstup, jednotka umožňuje standardní funkce jako je monitorování stavu dveří, narušení průchodu, použití neplatné karty, monitorování stavu zámku, monitorování ochranného kontaktu řídicí jednotky, třída identifikace 2 nebo vyšší a přístupová třída B oboje dle souboru ČSN EN 60839-11-1, Napájení 11,5 až 13,8V společně pro desku elektroniky i zámku.	68	ks	8 900,00 Kč	605 200,00 Kč	350,00 Kč	23 800,00 Kč
Terminál čtečky, čtečka	snímač čipových karet ve standardu MIFARE (13,56MHz).	79	ks	8 790,00 Kč	694 410,00 Kč	250,00 Kč	19 750,00 Kč
Elektrický dveřní otvírač	signalizace stavu OTEVŘENÝCH nebo ZAVŘENÝCH dveří. trvalý provoz (denní režim) 11-13V DC, Odběr cívek 10-24V 130mA.	57	ks	4 560,00 Kč	259 920,00 Kč	630,00 Kč	35 910,00 Kč
Dveřní zavírač	dveřní zavírač s hřebenovou technologií certifikován s lomeným ramínkem L190, Pro požárně odolné a kouřotěsné dveře do šířky 1100 mm a váhy 80 kg	63	ks	2 300,00 Kč	144 900,00 Kč	560,00 Kč	35 280,00 Kč
Přídavný zdroj +AKU	přídavný zálohovaný napájecí zdroj EZS 13,8V DC/ min. 5A, včetně oceloplechové skříně s detekcí sabotáže, poruchy 230V, poruchy AKU,a prostorem pro akumulátor 40Ah. Provedení min. pro stupeň zabezpečení 2	10	ks	5 500,00 Kč	55 000,00 Kč	690,00 Kč	6 900,00 Kč
SOS komunikátor	bezpečnostní interkom pro nouzovou komunikace, automatické nastavení hlasitosti, reproduktor 10W, podsvícené tlačítko, podpora SIP protokolu, vzdálená správa, 2x NO/NC výstup na externí zařízení	13	ks	11 260,00 Kč	146 380,00 Kč	580,00 Kč	7 540,00 Kč
Handsfree odpovídací komunikační jednotka	podpora HD aoudia, 7" dotykový displej, podpora zobrazení videa z externích kamer, informace o zmeškaném hovoru, vzdálená správa	1	ks	14 600,00 Kč	14 600,00 Kč	630,00 Kč	630,00 Kč
Turniket	trnový turniket s trubkovou konstrukcí, mód oboustranného průchodu, výška 1,6m	4	ks	58 000,00 Kč	232 000,00 Kč	6 400,00 Kč	25 600,00 Kč
Branka	nerozová křídlová branka se skleněnou výplní, Úhel otevření 0° - 270° pro každý směr	2	ks	33 000,00 Kč	66 000,00 Kč	5 900,00 Kč	11 800,00 Kč
Lapač karet	Lapač karet EXI-R automatický sběr návštěvnických karet při východu.	1	ks	63 000,00 Kč	63 000,00 Kč	4 890,00 Kč	4 890,00 Kč
Mechanická zábrana	nerozová konstrukce se skleněnou výplní, kotveno na chem kotvy	18	m	4 300,00 Kč	77 400,00 Kč	1 360,00 Kč	24 480,00 Kč
Oživení systému	Oživení systému na jednu čtečku	79	ks	0,00 Kč	0,00 Kč	125,00 Kč	9 875,00 Kč

SKV - kabeláž					0,00 Kč		
SKV	nízkofrekvenční kabel pro vnitřní instalace. Materiál vodičů Cu 6x0,5mm2, PVC izolace žil, elektrostatické stínění, PVC plášť, bílý nebo šedý	1490	m	6,44 Kč	9 595,60 Kč		0,00 Kč
SKV	datový 4 párový stíněný FTP kabel cat.5E, izolace PVC -, určeno pro propojení systémové sběrnice bez nutnosti přenosu napájení	2350	m	12,30 Kč	28 905,00 Kč		0,00 Kč
SKV	napájecí kabel pro vnitřní použití, materiál vodičů Cu, 2x1,5mm2, izolace PVC	480	m	7,90 Kč	3 792,00 Kč		0,00 Kč
SKV	napájecí kabel pro vnitřní použití, materiál vodičů Cu, 2x2,5mm2, izolace PVC	960	m	9,50 Kč	9 120,00 Kč		0,00 Kč
	Instalační materiál	1	kpl	11 890,00 Kč	11 890,00 Kč	28 000,00 Kč	28 000,00 Kč
CELKEM					2 422 112,60 Kč		234 455,00 Kč
DPH 21%					508 643,65 Kč		49 235,55 Kč

Televizní dohledový systém							
Zařízení	Popis	Počet	MJ	Cena/MJ	Cena/dodávka	Montáž/MJ	Cena/montáž
Server, záznamové zařízení	server s RAID systémem pro databázi - umožňuje nahrávat 64 IP kamer přes licenci CamConnect, komprese video MJPEG-H.264-H264CCTV-H265 HTTPS, 8 slotů RAID pro HDD max. 48TB, Rozhraní: DVI-D, DisplayPort, VGA, USB 3.0 2x, USB 2.0 Rozměr 482 x 133 x 543mm, 3U x 543mm pro 19" rack, napájení 110 - 240VAC/cca 240W, redundanční zdroje,	1	ks	320 600,00 Kč	320 600,00 Kč	6 800,00 Kč	6 800,00 Kč
Kamera vnitřní	Systémová Full HD IP kamera řady G-Cam3 minidome krytu s IR přísvitkem, Den/Noc s IR-C filtrem, 1/2.7" CMOS, objektiv 3 – 9mm/F1.2 vzdálené motorické ovládání zoomu a ostření, 16:9, Color 0,05Lx / BW 0,001Lx/32xSens-up, 1920x1080/30fps, ONVIF, AD, 100Mbit LAN, digitální vstup/výstup, napájení: PoE+ nebo 12VDC/24VAC max.20W, ,	31	ks	8 690,00 Kč	269 390,00 Kč	525,00 Kč	16 275,00 Kč
Kamera venkovní	Systémová Full HD IP kamera ve venkovním kompaktním provedení typu Bullet s IR přísvitkem, Den/Noc s IR-C filtrem, 1/2.8" CMOS 16:9, objektiv 3 – 9mm/F1.2, vzdálené motorické ovládání zoomu a ostření, Color 0,01Lx / BW 0,01Lx (50IRE/30pps), 1920x1080/50fps, digit. zoom x2 až x16, automatický BLC, WDR 96dB, Flip, Mirror, 2D/3D DNR, ONVIF, AD, 100Mbit LAN, digitální vstup/výstup, , dosvit LED max. 25m, napájení: PoE+ nebo 12-48VDC/24VAC max.cca 18W,	10	ks	13 090,00 Kč	130 900,00 Kč	1 625,00 Kč	16 250,00 Kč
PC Klientská stanice	CPU Intel® Core i7-5775C (3.3GHz, 6M, LGA1150, VGA) - (výkonnější CPU než 4790 a hlavně výkonnější integrovaná GK – důležité pro výpočetní výkon při streamování videa) ASUS Z97-P 8GB DDR3-1600MHz Kingston HyperX Fury Blue, 2x4GB, HP NVIDIA Graphics PLUS NVS 315 1GB PCIe x16 1xDMS-59 (2x DVI), SD 2, 5" 180GB Intel® 535 series SATAIII 7mm, 19" IPC case do racku, 480mm hloubka, černý, Fortron FSP500-60GHN 80PLUS BRONZE, black, bulk 500W, MS Win Pro 8.1 Win64bit Czech 1pk OEM DVD,	1	ks	22 350,00 Kč	22 350,00 Kč		0,00 Kč
LCD Monitor	LCD40" IPS 24/7, rozlišení 1920x1200, 16:9 podsvětlení typu IPS	2	ks	19 600,00 Kč	39 200,00 Kč	2 890,00 Kč	5 780,00 Kč
Oživení systému	Oživení systému na jednu kameru	41	ks	0,00 Kč	0,00 Kč	230,00 Kč	9 430,00 Kč

Televizní dohledový systém - kabeláž							
CCTV	nízkofrekvenční kabel pro vnitřní instalace. Materiál vodičů Cu 6x0,5mm2, PVC izolace žil, elektrostatické stínění, PVC plášť, bílý nebo šedý	600	m	6,44 Kč	3 864,00 Kč		0,00 Kč
CCTV	datový 4 párový stíněný FTP kabel cat.5E, izolace PVC -, určeno pro propojení systémové sběrnice bez nutnosti přenosu napájení	3200	m	12,30 Kč	39 360,00 Kč		0,00 Kč
CCTV	napájecí kabel pro vnitřní použití, materiál vodičů Cu, 2x1,5mm2, izolace PVC	0	m	7,90 Kč	0,00 Kč		0,00 Kč
CCTV	napájecí kabel pro vnitřní použití, materiál vodičů Cu, 2x2,5mm2, izolace PVC	0	m	9,50 Kč	0,00 Kč		0,00 Kč
	Instalační materiál	1	kpl	12 430,00 Kč	12 430,00 Kč	18 960,00 Kč	18 960,00 Kč
CELKEM					838 094,00 Kč		73 495,00 Kč
DPH 21%					175 999,74 Kč		15 433,95 Kč

Univerzální kabeláž							
Zařízení	Popis	Počet	MJ	Cena/MJ	Cena/dodávka	Montáž/MJ	Cena/montáž
Switch aktivní prvek	PoE switch 24/24+2 MNG, 24-portový switch PoE+ dle IEE802.af, 10/100Mbps , max proudový odběr 500W/19 Wport	2	ks	27 500,00 Kč	55 000,00 Kč	2 300,00 Kč	4 600,00 Kč
Záložní UPS	APC Smart-UPS RT 1000VA RM online	2	ks	16 600,00 Kč	33 200,00 Kč	690,00 Kč	1 380,00 Kč
Rack	19' rozvaděč stojanový 42U/800x800 skleněné dveře	2	ks	11 700,00 Kč	23 400,00 Kč	1 200,00 Kč	2 400,00 Kč
Systémový podstavec	Podstavec 800x800 s filtrem 1x	2	ks	1 425,00 Kč	2 850,00 Kč	450,00 Kč	900,00 Kč
Systémová police	Polička s perforací 1U/550mm, max.nosnost 40kg	4	ks	695,00 Kč	2 780,00 Kč	75,00 Kč	300,00 Kč
Rozvod 230V	RAB-PD-X07-A1,19' rozvodný panel,ČSN norma,8 zásuvek,	4	ks	1 368,00 Kč	5 472,00 Kč	75,00 Kč	300,00 Kč
Ventilační jednotka	Vent.j.spodní(horní)220V/60W 4 ventil. ,termostat RAL7035	2	ks	3 190,00 Kč	6 380,00 Kč	75,00 Kč	150,00 Kč
Osvětlovací jednotka	19' osvětlovací jednotka 1U RAL7035	2	ks	1 810,00 Kč	3 620,00 Kč	75,00 Kč	150,00 Kč
Kabelový kanál	Vertikální kabelový kanál - 1ks - 42U	4	ks	732,00 Kč	2 928,00 Kč	125,00 Kč	500,00 Kč
CELKEM					135 630,00 Kč		10 680,00 Kč
DPH 21%					28 482,30 Kč		2 242,80 Kč

Monitorovací řídicí systém, grafická nastavba							
Zařízení	Popis	Počet	MJ	Cena/MJ	Cena/dodávka	Montáž/MJ	Cena/montáž
SW LAT	administrační nástroj správy do 200 ADVANCED Admin	1	ks	20 000,00 Kč	20 000,00 Kč	2 580,00 Kč	2 580,00 Kč
SW LOW	pracoviště výkonného operátora (pro system ADVANC	1	ks	8 000,00 Kč	8 000,00 Kč	1 310,00 Kč	1 310,00 Kč
SW LGLE	editor grafických projektů	1	ks	29 900,00 Kč	29 900,00 Kč	1 100,00 Kč	1 100,00 Kč
SW LDE	data export Program pro export dat ze systému	1	ks	12 900,00 Kč	12 900,00 Kč		0,00 Kč
SW LAOM	modul automatických činností Služba	1	ks	10 900,00 Kč	10 900,00 Kč		0,00 Kč
	zadání dat prvku do grafické nastavby včetně vazeb	427	ks	0,00 Kč	0,00 Kč	110,00 Kč	46 970,00 Kč
	vytvoření primárních mapových podkladů (jeden půdorys)	8	ks	0,00 Kč	0,00 Kč	2 300,00 Kč	18 400,00 Kč
CELKEM					81 700,00 Kč		70 360,00 Kč
DPH 21%					17 157,00 Kč		14 775,60 Kč

Rekapitulace

Komplexní rekonstrukce bezpečnostních technologií - posílení zabezpečení		
System	Cena/dodávka	Cena/montáž
PZTS - poplachový zabezpečovací a tísňový systém	753 019,00 Kč	265 761,00 Kč
SKV - systém kontroly vstupu	2 422 112,60 Kč	234 455,00 Kč
Televizní dohledový systém	838 094,00 Kč	73 495,00 Kč
Univerzální kabeláž	135 630,00 Kč	10 680,00 Kč
Monitorovací řídicí systém, grafická nástavba	81 700,00 Kč	70 360,00 Kč
CELKEM	4 230 555,60 Kč	654 751,00 Kč
DPH 21%	888 416,68 Kč	137 497,71 Kč
CELKEM s DPH	5 118 972,28 Kč	792 248,71 Kč
CELKEM s DPH		5 911 220,99 Kč