

# DIPLOMOVÁ PRÁCE

Obor studia:

**Technická a informační výchova  
a anglický jazyk se zaměřením na vzdělávání**



## **Technologie zajišťující bezpečnost domácnosti**

*Safety and security technologies for households*

Autor: Bc. Marek Šnapka  
Univerzita Palackého v Olomouci  
Pedagogická fakulta

Olomouc, 2017

Prohlašuji, že jsem tuto práci vypracoval samostatně a s využitím zdrojů uvedených v příloženém seznamu.

V Olomouci dne 18.4.2017.

Marek Šnapka

.....

## Poděkování

Na tomto místě bych chtěl poděkovat mnoha lidem, stáli na pozadí při vzniku této práce.

Jmenovitě bych rád poděkoval:

- Ing. Čestmíru Serafinovi, Dr. Ing-Paed IGIP za odborné vedení této práce;
- Ing. Břetislavu Ulitzkovi za odborné vedení v oblasti instalací a norem;
- Mgr. Petru Volákovi za konzultace v oblasti datových sítí;
- Ing. Arnoštu Kleinovi za konzultace v oblasti školního managementu;
- Mgr. Pavlu Vojkůvkovi za konzultace v oblasti správy sítí;
- Mgr. Zdeňku Navrátilovi za konzultace v oblasti školního managementu;
- Mgr. Vilému Lukášovi za jeho přínosné poznatky v oblasti správy sítí;
- Pavlu Navrátilovi za přínosné poznatky v oblasti praktických instalací slaboproudu;
  
- dále společně:
  - Intelek za konzultace v oblasti fyzické vrstvy datových sítí;
  - SIDIT (jmenovitě Josefovi Sivkovi) za konzultace v oblasti telefonních systémů;
  - Joyce za konzultace v oblasti VoIP technologií;
  - Jablotron za umožnění účasti na školeních EZS a domovní automatizace a poskytnutí souhlasu k použití technických informací z manuálů k výrobkům;
  - Variant Plus za umožnění účasti na školeních EZS, SKS a CCTV

Zvláštní poděkování patří dále mé rodině a přátelům za mentální podporu v době tvorby.

Všem jmenovaným lidem bych rád vyjádřil svůj vděk za čas a úsilí, které mi věnovali.

## ANOTACE

<b>Jméno a příjmení:</b>	Bc. Marek Šnapka
<b>Katedra:</b>	Katedra technické a informační výchovy
<b>Vedoucí práce:</b>	Ing. Čestmír Serafín, Dr. Ing-Paed IGIP
<b>Rok obhajoby:</b>	2017

<b>Název práce:</b>	Technologie zajišťující bezpečnost domácnosti
<b>Název v angličtině:</b>	Safety and security technologies for households
<b>Anotace práce:</b>	Práce se zabývá analýzou metod zabezpečení domácností a budov a jejich aplikací v prostředí českého školství. Dále nahlíží na aktuální možnosti a stav vybavení školních budov elektronickými systémy a to s přihlédnutím k denní provozní realitě základních a středních škol v České republice. Dokument může posloužit jako referenční manuál pro jednotlivce, kteří se chtějí zorientovat v možnostech zabezpečovacích technologií, dále také pro zaměstnance škol při snaze zorientovat se v možnostech složitěho oboru IT, popř. může posloužit zřizovatelům škol pro načerpání inspirace při plánování jejich dalšího rozvoje po stránce technické i odborně pedagogické.
<b>Klíčová slova:</b>	bezpečnost, systémy, zabezpečovací, požární, vstupní, kamery, automatizace, budovy, elektronika, sítě, telefony, domácnosti, školy
<b>Summary in English:</b>	This writing descriptively analyses current methods of securing households and larger facilities, analyses the current possibilities and level of implementation of various electronic systems applicable for use in households and school buildings. The writing can be utilized as a reference for individuals wanting to get themselves oriented in wide possibilities of available security systems or for management staff of the Czech schools who would like to get quickly oriented in the commonly problematic field of information technologies. It also can be used by the school founders to find inspiration for future development of the managed schools in the fields of technical and pedagogical innovations.
<b>Keywords in English:</b>	security, safety, systems, alarms, fire, entrance, CCTV, automation, facilities, households, schools, electronics, networks, phones
<b>Přílohy vázané v práci:</b>	Příloha 1: Směrové detekční charakteristiky PIR detektorů  Příloha 2: Metodické doporučení k bezpečnosti dětí, žáků a studentů ve školách a školských zařízeních – minimální standard bezpečnosti  Příloha 3: Vyjádření a doporučení ÚOOÚ k možnosti instalovat kamerový systém v prostorách školy
<b>Rozsah práce:</b>	140 stran
<b>Jazyk práce:</b>	čeština

# Obsah

Úvod.....	7
<b>TEORETICKÁ ČÁST.....</b>	<b>8</b>
<b>1 Historický kontext elektronizace českého školství.....</b>	<b>8</b>
<b>2 Technická specifika jednotlivých technologických celků.....</b>	<b>12</b>
2.1 Klíčové infrastrukturní systémy.....	12
2.1.1 Strukturované kabelážní systémy.....	12
2.1.2 Telefonie.....	19
<i>Analogové telefonní sítě.....</i>	<i>19</i>
<i>VoIP.....</i>	<i>20</i>
<i>Ústředny.....</i>	<i>21</i>
<i>Telefonní terminály.....</i>	<i>23</i>
2.1.3 Datové sítě.....	26
<i>Metalické sítě.....</i>	<i>26</i>
<i>Bezdrátové sítě.....</i>	<i>29</i>
<i>Počítače.....</i>	<i>32</i>
<b>3 Bezpečnostní a dohledové systémy.....</b>	<b>33</b>
3.1 Elektronické zabezpečovací systémy.....	33
3.1.1 Detekce.....	34
<i>Pohybové detektory.....</i>	<i>36</i>
<i>Magnetické detektory.....</i>	<i>38</i>
<i>Ostatní plášťové detektory.....</i>	<i>39</i>
<i>Environmentální detektory.....</i>	<i>40</i>
3.1.2 Ovládání.....	40
3.1.3 Analýza.....	42
3.1.4 Komunikace.....	43
3.1.5 Řízení programovatelných výstupů.....	45
3.1.6 Shrnutí oddílu.....	47
3.2 Elektronické vstupní systémy.....	47
3.3 Kamerové systémy.....	50
3.4 Elektronické požární systémy.....	58
3.5 Monitoring technologických celků.....	61
<b>4 Doplnkové a komfortní systémy.....</b>	<b>62</b>
4.1 Místní rozhlas.....	62
4.2 Osvětlení.....	63
4.3 Topení a vzduchotechnika.....	73
4.4 Informační systémy školy.....	77
4.5 Systémová integrace.....	85
<b>5 Co přinese budoucnost?.....</b>	<b>87</b>
<b>APLIKAČNÍ ČÁST.....</b>	<b>92</b>
<b>I. Obecné poznatky.....</b>	<b>92</b>

<b>II. ICT management.....</b>	<b>93</b>
<b>III. Datová infrastruktura.....</b>	<b>96</b>
<b>IV. Bezdrátové sítě.....</b>	<b>105</b>
<b>V. Datové služby.....</b>	<b>108</b>
<b>VI. Počítače.....</b>	<b>110</b>
<b>VII. Telefonie.....</b>	<b>113</b>
<b>VIII. Elektronické zabezpečovací systémy.....</b>	<b>115</b>
<b>IX. Elektronické vstupní systémy.....</b>	<b>116</b>
<b>X. Kamerové systémy.....</b>	<b>117</b>
<b>XI. Ostatní elektroinstalace.....</b>	<b>118</b>
<b>XII. Zateplení a větrání.....</b>	<b>120</b>
<b>Závěr.....</b>	<b>122</b>
<b>Využití zdroje.....</b>	<b>123</b>
<b>Přílohy.....</b>	<b>128</b>

# Úvod

Cílem práce je analyzovat technologie a metody přispívající k zabezpečení a technologickému zhodnocení objektů a teoretické poznatky prokázat na průzkumu v oblasti českého školství.

Text v teoretické části by měl sloužit jako referenční materiál pro ty, kdož se chtějí zorientovat ve sféře zabezpečovacích a jejich doplňkových technologií nejen pro domácnosti, ale i jiné budovy. Může rovněž posloužit čtenářům, kteří mají zájem využít tyto poznatky v praxi a prostřednictvím těchto technologií zajistit modernost prostředí při projektování a realizaci novostaveb, zvýšit úroveň komfortu jejich obyvatel a pozvednout celkovou úroveň percepce prostředí z pohledu jejich obyvatel či návštěvníků. Teoretické poznatky jsou s přiměřenou mírou didaktické transformace demonstrovány a popisovány na prostředí škol, jelikož se školní budovy nabízejí jako vynikající popisné prostředí, u nějž je předpoklad, že se zde většina popsaných systémů bude reálně vyskytovat, že jej bude každý čtenář důvěrně znát a s nímž má autor praktické zkušenosti. Zavedení opatření navrhovaných v této práci má kromě zvýšení bezpečnosti také potenciál snížit náklady na provoz budov a ať už ve školství či jiných organizacích zvýšit efektivitu jak organizačních, tak pracovních (ve školství edukačních) procesů. Navrhovaná opatření také mohou zlepšit spokojenost pracovníků a návštěvníků v prostředí budov a zlepšit renomé dané organizace. Ve školství se toto může projevit větším zájmem o školu nejen ze strany žáků, ale i kvalitních pedagogů, což může prostřednictvím řetězového efektu zlepšit kvalitu školy, její vnímání u veřejnosti a úspěšnost absolventů vlivem lepších možností výběru vhodných kandidátů pro studium.

V praktické části je prostřednictvím kvalitativního šetření na dvou školách, které představují perfektní demonstrační prostředí, představena kazuistika reálného rozvoje a analýzy potenciálu pro další rozvoj popisovaných systémů. Část rovněž představuje praktické problémy při realizaci již hotových projektů a poskytuje tak čtenáři praktické informace upozorňující na situace vyplývající leckdy až reálného provozu.

# TEORETICKÁ ČÁST

Valná většina obyvatel ČR vlastní v roce 2017 mnoho elektronických zařízení, počínaje mobilními telefony, přes tablety, routery, notebooky až po chytré televize s připojením na internet, HiFi systémy ovládané přes Bluetooth, navigace, inteligentní stropní svítidla ovládaná blikáním LED diody na smartphonu, až po kávovary, pračky nebo autorádia s NFC. Trh je koncentrován na obchod se spotřební elektronikou, zatím co informace o profesionálních systémech, metodách efektivní a bezpečné správy nebo informace o tom, jak vybrat kvalitní produkty, zůstávají laickou veřejností opomíjeny. O to drastičtější následky může mít pozdější konfrontace laika se ziskuchtivým podnikatelem, kterého si zákazník platí pro správu systémů v jeho vlastnictví.

Následující kapitoly mají za cíl seznámit čtenáře s technologickými celky používanými v době psaní práce pro elektronizaci budov, nastítnit praktické možnosti jejich využití ve sféře českého školství a definovat následně možné směry jejich rozšiřování směrem k domácnostem. Cílem následujících kapitol by mělo být připomenutí celkem běžných, avšak často skrytých a tudíž uživateli přehlížených, popř. z různých důvodů dosud nezavedených systémů, které dokáží buď usnadnit rutinní práci a šetřit tak čas i náklady, popř. uspořit náklady přímo.

## ***1 Historický kontext elektronizace českého školství***

S rozvojem společnosti pocít'ují školy na území České republiky zvýšený tlak na rozvoj elektronických systémů. Příčina požadavků na elektronizaci škol spočívá primárně v digitální revoluci, která se v českých zemích výrazněji projevuje přibližně od přelomu tisíciletí. Za touto společenskou revolucí stojí primárně masivní rozvoj technologií, které umožnily levně produkovat výkonná výpočetní zařízení založená na polovodičích.

Mnozí z nás mají ještě v živé paměti počátky mobilních telefonů, osobních počítačů ve stolní či mobilní podobě, přechod z magnetofonů a VHS kazet na CD, DVD a nakonec jejich postupný odsun do pozadí zájmu s nástupem modernějších technologií a primárně rozvojem on-line světa.



S rozvojem litografických procesů docházelo od počátku devadesátých let dvacátého století k rapidnímu růstu výpočetního výkonu výpočetních jednotek (ať už procesorů, koprocessorů nebo třeba grafických čipů) a zlevňování jejich výroby. Tento jev měl několik důsledků.

1. Nejprve firmy a později i domácnosti si mohly dovolit koupit osobních počítačů.
2. Počítače se staly běžným pracovním nástrojem v práci.
3. S rozvojem informační gramotnosti obyvatelstva se počítače staly běžnou součástí domovů.
4. Ustálil se trh a oddělily se perspektivní platformy od neperspektivních. Trh s ICT se zúžil na majoritní hráče a začal se vysoce specializovat a standardizovat, ke slovu se dostaly kompatibilní platformy s intuitivním ovládáním (architektura x86, později x64). Korporace začaly pohlcovat větší vývojářské a výrobní společnosti, redukoval se počet značek a docházelo k integraci technologií do majoritních produktů. Tempo inovací raketově vzrostlo.<sup>1</sup>
5. S nárůstem syntetického výpočetního výkonu bylo možné využít i dalších zařízení, která otevřela majitelům počítačů bránu do světa multimédií. Výrazného rozvoje se tak dočkaly např. grafické karty, střížny, TV tunery, ad. Počítače se tak staly nejen pracovním nástrojem, ale i prostředkem zábavy.
6. S poklesem výrobních nákladů se výrazný rozvoj odehrál i na poli propojování jednotlivých počítačů. Původně vojenské a akademické sítě se tak staly základem pro rozvoj mezinárodního Internetu.
7. Mohutný rozvoj konektivity se stal základem pro spuštění nových typů služeb. Internet, do té doby poskytující majoritně služby jako e-mail a statické webové prezentace, vstoupil do éry sdílení souborů, živého streamování multimédií, video on demand a v poslední době dochází i k rapidnímu nástupu cloudových služeb – e-maily počínaje, hlídáním sítě konče.<sup>2,3</sup>

---

1 Historie počítačů: Od elektronky po internet. Živě [online]. 2011 [cit. 2017-04-13]. Dostupné z: <http://www.zive.cz/clanky/historie-pocitacu-od-elektronky-po-internet/sc-3-a-147343>

2 The '90s: science and technology: When the Internet first took hold of our lives. National Geographic [online]. 2014 [cit. 2017-04-13]. Dostupné z: <http://channel.nationalgeographic.com/the-90s-the-last-great-decade/articles/the-90s-science-and-technology/>

3 Technological Advances of the 90s. Bright Hub [online]. 2012 [cit. 2017-04-13]. Dostupné z: <http://www.brighthub.com/education/homework-tips/articles/123405.aspx>

8. S dalším rozvojem litografie a minimalizací výpočetního výkonu přišly ke slovu SoC (system-on-chip), což jsou zařízení integrující původně diskrétní zařízení (procesor, řadiče operační paměti i úložišť, grafické jádro, komunikační moduly, audio vstupy i výstupy, atp.). Tyto SoC se staly základem pro nástup éry mobilních zařízení ve všech podobách, jak je známe dnes. Digitální mobilita se stala běžnou součástí životů (hlavně mladých lidí chodících do škol), běžně jsou využívány smartphony, tablety, méně často i tzv. wearables (chytré hodinky, monitory tělesných funkcí, brýle pro rozšířenou realitu, atp.) nebo např. výkonné outdoor kamery, které by bez tohoto rozvoje nedisponovaly dostatečným výpočetním výkonem.<sup>4,5</sup>

Ani školám se tyto rozvojové trendy nevyhnuly... tedy jak kde. V oblasti informačních technologií můžeme ve školství pozorovat mezigenerační střet způsobený tím, že mladší generace s těmito zařízeními vyrostla, naučila se s nimi pracovat a rovněž aplikuje v životě odlišný přístup k práci s informacemi. Starší a často konzervativnější generace je však méně připravena přijmout obrovské množství změn za tak krátký časový úsek, poznat, kdy je potřeba se přizpůsobit, v čem a najít si mezi všemi těmi novinkami vlastní cestu. Výsledkem při nevyhnutelné konfrontaci je tak často neznalost jinak vysoce kvalifikovaných lidí, odborníků ve svém oboru. Velkou roli při vzdělávání pedagogických pracovníků však hraje ještě jeden velice významný faktor. Historický vývoj, financování a personální politika škol a z toho vyplývající atraktivita vzdělávací sféry pro odborníky v oblasti IT.<sup>6</sup>

České školy měly po roce 1989 plné ruce práce primárně samy se sebou – čekal je náročný přechod od komunistického jednotného školství k současnému stavu, během kterého se vedení škol muselo potýkat s náročnými změnami jak v oblasti pedagogické (kurikulární reformy) tak i organizační (financování, změna zřizovatele, rychlá dynamika změn z MŠMT v porevolučním období) a provozní (rekonstrukce 40 a více let nerekonstruovaných budov, změny technických a hygienických norem). Z těchto důvodů byla často odsunuta modernizace prezentační a výpočetní techniky na vedlejší kolej. Je rovněž důležité zmínit, že v devadesátých letech s otevřením hranic se v oblasti informačních technologií ve školském sektoru pohybovalo jen velmi málo kvalifikovaných pracovníků a potenciál jejich zaměstnání byl mizivý a to

---

4 A Brief History of SoCs. Semiwiki.com: The open forum for semiconductor professionals [online]. 2012 [cit. 2017-04-13]. Dostupné z: <https://www.semiwiki.com/forum/content/1586-brief-history-socs.html>

5 The why, where and what of low-power SoC design. Eetimes [online]. 2004 [cit. 2017-04-13]. Dostupné z: [http://www.eetimes.com/document.asp?doc\\_id=1276973](http://www.eetimes.com/document.asp?doc_id=1276973)

6 ZOUNEK, Jiří a Klára ŠEĎOVÁ. Učitelé a technologie: mezi tradičním a moderním pojetím. 1. vyd. Brno: Paido, 2009, 172 s. ISBN 978-80-7315-187-4.

primárně z ekonomických důvodů – kvalifikovaní odborníci byli v soukromém sektoru placeni násobně lépe. Když je člověk odborníkem přes určitou oblast IT, umí cizí řeč a je mobilní, české školství bývá poslední oblast, kam se tito lidé uchýlí s cílem budovat kariéru. Navíc, jak prokazuje praktická část této práce, stav, kdy si škola uvědomí, že potřebuje najít odborníka, ví, podle čeho si vybrat, a pokud jej najde, má jej z čeho zaplatit, je výjimečný dnes stejně jako dříve.

Jak však tyto lidi do praxe přitáhnout? Krom náležitého finančního ohodnocení vyhledávají školní síť'aři toto prostředí primárně pro časovou flexibilitu, kterou tato práce nabízí. Člověk tak může v rámci limitů (a pokud vše funguje ku spokojenosti všech) být svým vlastním páнем. Pokud má navíc za zády vedení, které jej podpoří v případě potřeby a které jej nebude nutit cítit se špatně, když je požádá o drahou techniku potřebnou pro jeho činnost, jistě se najde uchazeč, který tuto práci bude vykonávat poctivě a s odhodláním.

Pro vedení by mělo být naopak velice důležité, aby za uvolněné finance dostávalo od technika adekvátní služby, aby nebyly finance utráceny zbytečně a aby měl člověk ujasněnou dlouhodobou vizi rozvoje a byl ji schopen a ochoten pravidelně aktualizovat podle nových možností, které mu trh nabídne.

S přihlédnutím na ekonomickou konjunkturu ČR v době psaní této práce, snahu zlepšit financování českého školství a také z osobní zkušenosti autora lze soudit, že rozsáhlejšímu zájmu o řešení stavu výpočetní, prezentační a komunikační techniky ze strany škol dochází až v posledních třech až pěti letech. K efektivnímu investování veřejných prostředků je však zapotřebí více, než znalost pedagogiky, byť v oblasti ICT. Odbornost učitelů byt' středních odborných škol bývá většinou uživatelská a tito lidé zřídka mívají zkušenosti z pohledu systémového administrátora. Výchozím předpokladem pro psaní této práce byla zkušenost autora, kdy převzal ke správě ICT školu z rukou odvolaného rekvalifikovaného učitele dílen, jenž tuto oblast dostal dobré víře svěřenu jakožto učitel mající k oblasti v dané době nejbliže.

Ze zkušeností z praxí na školách základních a z workshopů a konferencí týkajících se ICT ve školství je autor rovněž obeznámen s faktem, že české školy si najímají ke správě odborníky jen výjimečně a to většinou k jednorázovým úkonům, nikoliv k systémovému budování školní infrastruktury. Proto vznikly tyto řádky, jenž měly za cíl nikoliv sepsat alibistickou práci s jediným cílem ji obhájit a zavřít do skříně, ale primárně s cílem sumarizovat poznatky autora z dosavadní praxe, rozvinout je a přinést kolegům ve školství zajímavé poznatky a postřehy, díky kterým budou moci investovat veřejné finance efektivněji, s jasnou vizí do budoucna a s cílem

zlepšit prostředí studijní a pracovní. Autor zastává názor, že v této oblasti je skryt velký potenciál a přináší návrhy na realizaci této myšlenky.

## **2 Technická specifika jednotlivých technologických celků**

Následující kapitola je rozdělena do dvou částí. První část je věnována elektronickým řešením, bez kterých si jak informační společnost, tak jiné chytré systémy jen těžko může představit běžné fungování. V části následující bude pak pozornost věnována systémům nadstavbovým, které dokáží těch infrastrukturních využít ke složitějším úkolům.

### **2.1 Klíčové infrastrukturní systémy**

#### **2.1.1 Strukturované kabelážní systémy**

V každé moderní budově školy by mělo být možné nalézt strukturovanou metalickou kabeláž. Řeč je konkrétně o jednotné fyzické vrstvě pro sdělovací zařízení, jako jsou např. datové sítě.

Strukturované kabelážní systémy (zkráceně SKS, setkat se lze i s pojmy „strukturovaná kabeláž“ či slangově „strukturka“) jsou dle definice uvedené v podkladech pro školení třebíčské firmy Variant Plus<sup>7</sup> „univerzální kabelážní rozvody v rámci budovy, které umožňují přenos digitálních a analogových signálů bez nutnosti další instalace speciálních kabelových rozvodů“.

Počátky rozsáhlejšího budování strukturovaných kabelážních systémů na školách se datují k roku 2001, kdy MŠMT spustilo v rámci svého projektu „Státní informační politika ve vzdělávání“ z dnešního pohledu kontroverzní projekt „Internet do škol“ (INDOŠ). Zamýšleným cílem tohoto projektu bylo rozdělit miliardu korun ročně mezi české školy za účelem podpory rozvoje informační společnosti v České republice prostřednictvím investic do rozvoje výpočetní techniky a datové infrastruktury právě ve školách. Pomineme-li fakt, že tato původně bohubilá iniciativa byla tehdejší politickou garniturou řádně okleštěna a tudíž

---

7 Strukturovaný kabelážní systém - příručka [online]. 2017, 48 s. [cit. 2017-04-06]. Dostupné z: [https://www.variant.cz/soubory-ve-skladu/Karty/Spol\\_Zarazene/01-MANU%C3%81LY%20CS/SKS%20prirucka%20-%20man-a4.pdf](https://www.variant.cz/soubory-ve-skladu/Karty/Spol_Zarazene/01-MANU%C3%81LY%20CS/SKS%20prirucka%20-%20man-a4.pdf)

se nedostalo na všechny školy, že část těch šťastnějších škol byla vybavena menším množstvím počítačů, než bylo plánováno (tudíž byl v této učebně často problém učit už jen polovinu třídy), z čehož se daly všechny označit i na tehdejší poměry za předražený šrot<sup>8,9</sup> (k čemuž se vyjádřil i ředitel oslovené ZŠ – během dvou let museli PC vyměnit; autor sám se na počítačích z tohoto projektu učil při studiu na gymnáziu a má dobře v paměti vyryty chvíle, kdy počítač na bázi Celeronu (s výkonem v té době nižším než o generaci starší Pentium III Tualatine) pravidelně zamrzal při snaze uložit rozepsaný dokument ve Wordu) a že tato snaha vyústila v tunelování 884 milionů korun za což padlo několik trestních oznámení a pokut, kdy stát ve výsledku pokutoval sám sebe<sup>10</sup>, můžeme říci, že byl částečně úspěšný. I přes všechna negativa<sup>11</sup> totiž tento projekt vedl jednak ke změně myšlení zodpovědných lidí na školách, kdy jejich vedení začalo vůbec pracovat s myšlenkou rozvoje strukturovaných sítí a elektronizace budov i samotného procesu výuky, rovněž však vyústil k připojení těchto škol do rychle se rozvíjející sítě Internet, o které do té doby slyšeli maximálně na univerzitách, v knihovnách a ve firmách. Tato politika, ač si to uvědomuje málokdo, má dalekosáhlé implikace až do dnešních dní.

V současnosti se totiž tyto dnes již zastaralé datové sítě začínají dostávat na hranice svých možností. Co se od dob, kdy spatřil světlo světa projekt INDOŠ změnilo, jsou aktivní prvky sítí. Co však zůstalo prakticky stejné a ještě nějakou dobu (10 let minimálně) stačit bude, jsou již existující kabelové rozvody vytvořené právě s příchodem projektu INDOŠ. Pro školy, které v dnešní době pociťují nutnost upgradu síťové infrastruktury, tak velmi často odpadá nebo se značně zlevňuje velmi nákladná část budování moderních datových sítí – povrchová montáž či zasekávání kabelových chrániček a tažení rozvodů.

S vývojem technologií se na trhu objevily strukturované systémy mající různé rozložení prvků sítě, rozdílnou topologii. Základními topologiemi datové a tudíž i kabelové infrastruktury jsou sběrnice, hvězda a kruh. V průběhu let se vývoj technologií ustálil a běžným standardem v oblasti datových sítí a strukturované kabeláže je rozvod do hvězdy realizovaný kabely tvořenými čtyřmi kroucenými dvojlinkami ve společné izolaci. Tato technologie SKS se ve světě ustálila jako vedoucí kvůli několika zásadním výhodám.

---

8 Internet ve školách: jak skončil byznys za 884 milionů korun. ITbiz.cz [online]. Štěpán Beneš, 2007 [cit. 2017-04-06]. Dostupné z: <http://www.itbiz.cz/internet-ve-skolach>

9 VLČKOVÁ, Gabriela. Internet do škol - analýza efektivnosti veřejného projektu. Brno, 2006. Masarykova Univerzita v Brně. Vedoucí práce Mgr. Jiří Špalek, Ph.D.

10 SIPVZ: Proč vlastně NKÚ podává trestní oznámení? EArchiv.cz [online]. Jiří Peterka, 2002 [cit. 2017-04-06]. Dostupné z: <http://www.earchiv.cz/b03/b0814002.php3>

11 INDOŠ story. Učitel'ské noviny [online]. 2003 [cit. 2017-04-13]. Dostupné z: <http://www.ucitelskenoviny.cz/?archiv&clanek=3752>

1. Netrpí výrazným snižováním propustnosti linky (uvažováno point-to-point bez extrémních případů velkých L2 domén) s přidáváním dalších zařízení do sítě (na což trpěly především sběrníkové sítě vlivem vzniklých vysílacích kolizí na sdíleném médiu).
2. Při poruše trasy jednoho koncového bodu funguje celá síť dále bez něj.
3. Využívá levné, jednoduše vyrobitelné a **univerzálně využitelné** kabely.
4. Lze jednoduše centralizovat správu, napájení, zálohování systémů, atp. do jediné lokality.
5. Pro odstranění závady člověk ví, kde je začátek a konec kabelu, nemusí procházet celou trasu vedení.
6. Budoucí upgrady jsou většinou řešitelné pouhou výměnou aktivního prvku, kabeláž zůstává.<sup>12</sup>

Hlavní výhodou SKS na bázi čtyř kroucených párů je univerzálnost využití takového rozvodu. Nemusí být totiž použity pouze na data, ale je velice jednoduché využít takovýto systém např. pro spojení analogových telefonů s telefonní ústřednou, čidel zabezpečovacího systému s ústřednou EZS (viz 4.1), otevírání zámků, zvonek, napájení routerů, kamer, přístupových bodů bezdrátových sítí, ovládání výsledkových tabulí, spínání topení, připojování environmentálních čidel, atp., což činí toto řešení ideálním z pohledu užitné hodnoty systému s výhledem do budoucnosti.

SKS je v současnosti vhodné budovat nejlépe s využitím kabeláže cat. 5e, popř. cat. 6a, dle finančních možností projektu. Kategorie kabeláže jsou popsány v sadě norem TIA/EIA-568<sup>13</sup> s poslední aktualizací v roce 2014. V těchto dokumentech se můžeme dočíst o normativních elektrických vlastnostech, které musí kabeláž dané kategorie splňovat. Výše zmíněné kategorie 5e a 6a jsou používány prakticky výhradně – kategorie („6“ a „7“) nemají s ohledem na poměr ceny k výkonu význam. Mezi kategorií 6 a 6a je funkční rozdíl majoritní a cenový minoritní a kabely cat. 7 se využívají výhradně ve zvláštních případech a jsou dražší.

Kvalitní kabely kategorie 5e jsou tvořeny čtyřmi kroucenými dvojlínkami tloušťky 24 AWG (stupnice American wire gauge), což je převedeno na metrický průměr 0,511 mm, v průřezu 0,205 mm<sup>2</sup> ve společné izolaci o tloušťce cca. 0,25 mm. Frekvence, kterou tuto kabely

---

12 KÁLLAY, Fedor a Peter PENIAK. Počítačové sítě a jejich aplikace: LAN / MAN / WAN. 2. aktualiz. vyd. Praha: Grada, 2003. ISBN 80-247-0545-1.

13 TIA Standard: Balanced Twisted-Pair Telecommunications Cabling and Components Standards. Innowave.com [online]. Arlington, VA, U.S.A.: Telecommunications industry association, 2009 [cit. 2017-04-06]. Dostupné z: <http://innovave.com/wp-content/uploads/2016/01/TIA-568-C.2.pdf>

musí zvládnout přenést je 100 MHz, maximální délka spoje činí 100 m. Tato kategorie se využívá pro většinové běžné účely – je cca. o 30% levnější, než kategorie 6, lépe se s ní pracuje (menší tuhost) a počítá s datovým provozem o maximální rychlosti 1/1 Gbps při použití v běžných Ethernet sítích definovaných standardem 802.3 a jeho dodatky souvisejícími s linkovou vrstvou. Kategorie 5e vychází historicky z kategorie 5, která byla určena výhradně pro 100Mbit sítě, avšak s ohledem na ekonomické důvody byla po nátlaku výrobců povolena i pro gigabitový ethernet. V praxi však může být reálná propustnost gigabitového spoje snížena. Pro případy kvalitního gigabitového ethernetu se využívá kabeláž cat. 6a.

Kvalitní kabely kategorie 6 využívají vodiče tloušťky 22 AWG, (průměr 0,644 a průřez 0,326 mm<sup>2</sup>), tloušťka izolace je shodná s cat. 5e, navíc ale přibyl oddělovací kříž držící jednotlivé páry v určité vzdálenosti od sebe. Tyto kabely garantují přenosové frekvence až do 250 MHz a lze je využít pro již zmiňovaný gigabitový ethernet na vzdálenost do 100 metrů, rovněž jsou však určeny pro 10Gb ethernet na vzdálenost 33-50 metrů. Kategorie 6a je oproti cat.6 dražší jen cca. o desetinu, nabízí však dvojnásobnou šířku pásma oproti cat. 6 (celých 500 MHz). Tyto kabely jsou však stíněné a je nutné využít pro jejich instalaci odpovídající příslušenství (stíněné patch panely, keystone, vše dobře uzemnit, atd.). Kabely kategorie 7 garantují šířku pásma do 600 MHz se stíněním každého páru. Určeny jsou pro 10Gbit Ethernet na maximální vzdálenost 100 metrů (čili vysokorychlostní páteřní linky). Místo nasazení kabeláže cat. 7 je už na zvážení, zda nebude levnější využít kabeláže optické.

Kabely dále dělíme dle materiálu, ze kterého je vyrobena jeho vnější izolace. Běžně se lze setkat s třemi druhy: PVC, LSZH a PE. Tyto tři zkratky značí polyvinylchlorid, low-smoke-zero-halogen a polyetylen. PVC a LSZH kabely se používají pro vnitřní instalace, kdy PVC kabely by se měly používat výhradně pro horizontální instalace, popř. vedení v instalačních trubkách za účelem eliminace šíření případného požáru mezi patry. LSZH kabely jednak obsahují zpomalovače hoření a když už hoří, nejdou z nich toxické zplodiny, jako v případě levnějšího PVC. To při hoření uvolňuje hustý černý dým ztěžující orientaci osob při evakuaci, chlorovodík způsobující leptání sliznic a jiné toxické plyny. Polyetylenové kabely se využívají výhradně pro venkovní instalace, kde je potřeba zvýšená odolnost proti UV záření a mechanickému namáhání. Tyto kabely jsou velmi tuhé, rády se krouť a jejich instalace je tak náročnější, než v případě výše uvedených typů.<sup>14</sup>

---

14 LSZH and PVC cables. Black Box network services [online]. Hallbergmoos, Německo, 2009 [cit. 2017-04-06]. Dostupné z: <https://www.black-box.de/en-de/page/27275/Resources/Technical-Resources/Black-Box-Explains/Copper-Cable/lshz-and-pvc-cables/>

Strukturovaná kabeláž nese své jméno nejen podle toho, jakým způsobem je rozvedena po budově, ale také kvůli metodám, jakými se ukončuje – typicky je na jednom konci ukončena rozvaděčem a na druhém zásuvkou, popř. konektorem (např. přípojky pro kamery či WiFi AP).

Rozvaděče (anglicky sing. „rack“; pl. „racks“) slouží jako centrální uzly sítí s hvězdicovou topologií. Mají standardizované rozměry, pro účely datových center a slaboproudých rozvodů se však běžně využívají pouze dva rozměry – 19“ a méně běžnější 10“. Tyto rozměry v palcích definují šířku rozvaděče. Výška rozvaděčů se udává v jednotkách RU, což je zkratka pro „rack unit“ vyjadřující míru 4,45 cm (RU se běžně zkracuje jen na U). Standardní výška průmyslového rozvaděče a zároveň největší běžně dostupné provedení je 42U. Na trhu jsou dostupná různá provedení rozvaděčů, lišící se hlavně parametry jako hloubka, použitý materiál, provedení stojanové vs. závěsné, čelo průhledné vs. plechové, příprava na klimatizační jednotku, koupit se dají i rozvaděče s pokročilým mechanickým zabezpečením.

Do rozvaděčů se montují nejrůznější moduly. Těmi nejdůležitějšími jsou tzv. patch panely. Jedná se o přípravek sloužící k efektivnímu ukončení slaboproudé kabeláže za účelem zjednodušení manipulace a jejího propojování. Z čelní strany je patch panel osazen porty příslušného typu (nejčastěji téměř univerzálními RJ-45) a ze zadní strany slouží k vyvázání kabeláže – slouží tak jako rozhraní mezi kabely a standardizovanými přípojnými body. Patch panely mohou být modulární, tzn. že umožní osadit tzv. keystoney a sestavit si tak panel z různých konektorů či různobarevně, nebo již fixně osazené. V praxi se lze častěji setkat s fixně osazenými panely, v případě nových instalací již výhradně s vyvazovací lištou, která, oproti starším typům, drží kabely pevně ukotvené k panelu i v případě mechanického namáhání tahem. U starších modelů docházelo nezdědky k nechtěnému vytrhnutí kabelu v případě manipulace se svazkem. Pro 19“ racky se využívají nejčastěji 24-portové patch panely – více portů se nevyužívá – není je kam umístit a větší switche se stejně nevyrábí. K dostání jsou však panely s menším počtem portů (12/16/18), výjimečně i 50-portové RJ-45 panely pro telefonní ústředny, které však nabízí pouze 2-4 piny na port.

Kromě patch panelů se do pozic v rozvaděči osazují také např. aktivní síťové prvky (switche, routery, firewally), optické vany (ukončení optických spojů), servery, KVM switche, disková pole, media converter backplanes, atd. Standardizované racky v mobilním provedení rovněž nachází své uplatnění v efektové a audio-technice.<sup>15</sup>

---

15 Rack IMG Stage Line MR-720. Muziker.cz [online]. 2017 [cit. 2017-04-13]. Dostupné z: <https://www.muziker.cz/img-stage-line-mr-720>

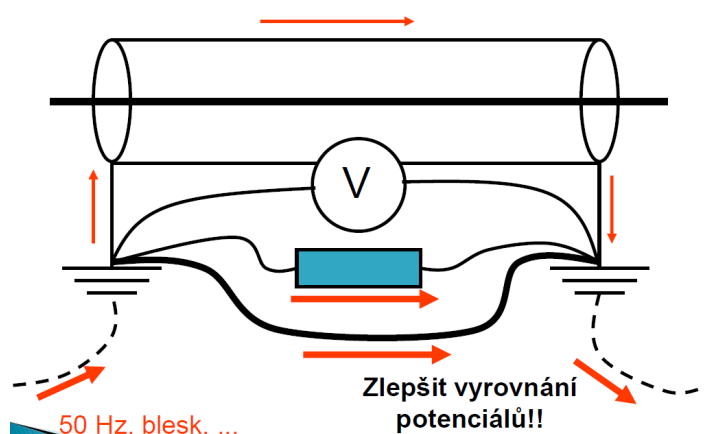


Na druhém konci kabelu, než je rozvaděč, nalezneme samotné přípojné body. Tyto bývají realizovány prostřednictvím zásuvek. Zásuvek existuje na trhu spousta typů, výběr se v dnešní době řídí prakticky jen požadovaným designem a provedením. Zásuvky se vyrábí v provedeních pro zapuštění do krabiček pod omítkou a povrchové pro instalace pomocí lišt. Jak již bylo uvedeno výše, hlavní výhodou těchto fixně umístěných přípojných bodů spojených kabeláží s rozvaděčem SKS je jejich univerzalita a potenciál využití v budoucnu při případné změně technologie. Např. do kabinetu je tak možné přivést jak data pro počítače, tak i např. analogový telefon, kameru, čtečku čipů nebo otevírač dveří. Pro instalaci kterékoliv této technologie stačí zařízení připojit do připravené univerzální zásuvky (RJ-45) a její druhý konec propojit v rozvaděči s příslušným zařízením (taktéž se vyvádí na porty, pak je možno využít obyčejných síťových kabelů pro přímé spojení).

Zvláštní situace může nastat v případě, že je potřeba využít stíněných kabelů. Tento požadavek vzniká primárně ve dvou případech – buď je potřeba vést datové linky v prostředí s vysokou mírou EMI (elektromagnetické rušení), popř. v prostředí, kde je do budoucna plánován přechod na vysokorychlostní 10Gbit síť. Stínění v podobě kovem potažené fólie obalující buď všechny páry najednou (cat. 6a) nebo jednotlivé páry (cat. 7) je elektricky spojeno se zemnicím vodičem (drain wire) vedoucím uvnitř kabelu. Na koncích kabelů je pak zemní vodič spojen s obvodově vodivými konektory zasouvány do příslušně upravených portů. Norma ČSN EN 50310 ed. 3 říká, že zemnicí kabel má být uzemněn na obou koncích linky. Existuje však jeden velmi podstatný faktor, který nebere tato norma v potaz a kvůli něž se montážní technici od této normy často cíleně odchylují – bludné proudy a potenciál mezi dvěma lokalitami. Zemnění na dvou bodech totiž může zkvalitnit kvalitu linky jen za podmínky, že jsou obě země přivedeny z jediného bodu, že v síti neexistují další zemnění a že mezi těmito body existuje jen minimální přechodový odpor. Pokud nejsou tato pravidla splněna, hrozí, že mezi dvěma zemnicími body bude existovat elektrický potenciál vedoucí k průtoku proudu stíněním. Obzvláště náchylné jsou na tento jev lokality pracující s vysokovýkonovými elektrickými stroji, např. hutě, strojírenské závody či železniční nádraží. Dle Ing. Ulitzky je zde šance, že tepelné účinky bludných proudů vzniknuvších v utvořené zemní smyčce mohou vzhledem k jejich potenciální velikosti způsobit i požár. Údajně sám podobný případ, kdy po nahlášení poruchy zákazníkem v montážní hale našel protavený datový kabel a podle zkušeností techniků přítomných na certifikačním školení o metalických a optických sítích firmy Variant Plus je toto častým jevem. Z tohoto důvodu je na těchto lokalitách často cíleně používáno uzemnění jen na jednom konci kabelu, což bohatě postačuje a nedochází tak k toku

vyrovnávacích proudů. Kvalitní popis s výše uvedenou ilustrací uvádí i zdroj, česká firma zabývající se výrobou instalačního materiálu pro slaboproudé instalace.<sup>16</sup>

Oboustranné zemnění => vyrovnávací proud!!



Ilustrace 1: Schéma vyrovnávacích proudů

Stíněné datové kabely se označují dle níže uvedené ilustrační tabulky<sup>17</sup>, ve které si lze dobře povšimnout výrazných diskrepancí mezi normou ISO/IEC 11801 a běžně používanými komerčními názvy. Z tohoto důvodu je v praxi vhodné si před koupí materiálu ověřit informace do posledního detailu.

Common industry abbreviations for cable construction

Industry acronyms ⇅	ISO/IEC 11801 name ⇅	Cable shielding ⇅	Pair shielding ⇅
UTP	U/UTP	None	None
STP, ScTP, PiMF	U/FTP	None	Foil
FTP, STP, ScTP	F/UTP	Foil	None
STP, ScTP	S/UTP	Braiding	None
SFTP, S-FTP, STP	SF/UTP	Braiding, foil	None
FFTP	F/FTP	Foil	Foil
SSTP, SFTP, STP PiMF	S/FTP	Braiding	Foil
SSTP, SFTP	SF/FTP	Braiding, foil	Foil

16 PANTŮČEK, Edmund. Poznatky z provádění kontrol elektrické instalace [online]. Praha: Schrack.cz, 2016, s. 29 [cit. 2017-04-06]. Dostupné z: [https://www.schrack.cz/fileadmin/f/cz/Bilder/Infodny\\_2016/Prezentace\\_Infodny/Nejcastejsi\\_chyby\\_v\\_elektroin\\_stalacich\\_Pantucek.pdf](https://www.schrack.cz/fileadmin/f/cz/Bilder/Infodny_2016/Prezentace_Infodny/Nejcastejsi_chyby_v_elektroin_stalacich_Pantucek.pdf)

17 Twisted pair. Wikipedia.org [online]. 2017 [cit. 2017-04-06]. Dostupné z: [https://en.wikipedia.org/wiki/Twisted\\_pair](https://en.wikipedia.org/wiki/Twisted_pair)

## **2.1.2 Telefonie**

Velice důležitým technologickým celkem zajišťujícím spojení školy s okolním světem je veřejná telefonní síť. Kdo všechno disponuje ve škole telefonním přístrojem je samozřejmě velmi variabilní, ale většinou jsou to ředitel, zástupce ředitele, sekretářka, účetní a učitelský sbor. Hodně záleží na rozložení místností ve škole a zda jsou učitelé koncentrováni do jedné sborovny či zda jsou rozmístěni do více kabinetů – v tom případě je zvykem umisťovat telefon do každého kabinetu tak, aby byl učitel dostupný nejen pro vedení a rodiče, ale hlavně pro své kolegy.

Hlasové komunikační systémy prodělaly a ještě stále prodělávají divoký vývoj přímo úměrně jdoucí s technologickým pokrokem mobilních technologií. Následující řádky si kladou za cíl shrnout nejdůležitější milníky tohoto vývoje podstatné pro aplikaci ve školním prostředí.

### **Analogové telefonní sítě**

Z minulého století se v organizacích nezdálo dochovaly analogové telefonní sítě. Tyto sítě mají několik variant provedení.

Úplně nejzákladnější provedení je přímé napojení telefonního přístroje do veřejné telefonní sítě. Tato varianta umožňuje využití pouze jediného telefonního čísla a umožňuje komunikaci pouze z jediného místa, popř. ze dvou v rámci podvojně linky. Využití podvojně linky však přináší značné nevýhody, mezi něž patří hlavně možnost odposlechu probíhajícího hovoru z druhé linky. Je rovněž možné se setkat s řešením, kdy do školní budovy bylo zavedeno více přímých linek a ty byly následně rozvedeny do příslušných lokalit. Toto řešení je využíváno hlavně na školách malých, s ohledem na nízké pořizovací náklady. Hlavní nevýhodou jsou dnes vysoké náklady provozní (tarifní) v porovnání s modernějšími službami.

Složitějším provedením analogových telefonních sítí je využití lokální školní ústředny. Toto řešení přináší vyšší investiční náklady, ve větších školách jsou však tyto systémy nutností kvůli rozlehlosti školního areálu a z toho vyplývající roztržiténosti zaměstnanců. Telefonní sítě s ústřednou mají dva hlavní účely. V první řadě slouží k rychlé a efektivní komunikaci mezi zaměstnanci v organizaci – učitelé tak mohou zvednutím sluchátka a naťukáním krátkého čísla ihned mluvit s kolegy v jiných kabinetech, vedením školy, jídelnou, knihovnou, atp. Systém může fungovat buď na analogové nebo na digitální bázi. Staré analogové ústředny mají přivedeny fyzicky samostatné telefonní linky (1 kabelový pár = 1 linka), přičemž slouží pouze jako komplikovanější kabelový přepínač. Tento systém však již tehdy řešil velkou neefektivitu

využití linek v případě nevyužití pobočkové ústředny. Za podmínky že měla organizace 50 místních klapků bylo nutné do ústředny nutné dovést 50 kabelových párů, což je již samo o sobě velmi nákladné a za podmínky, že linka nebyla takto dimenzována již při stavbě (tzn. pokud jde o rekonstrukci), bylo by nutné vyměnit kabelové vedení mezi ústřednou místní a ústřednou operátora, což by znamenalo provést výkop, uložit do něj velmi drahý kabel a částečně rozsekat i budovu, což je nereálné. I tak však jsou z dnešního pohledu tyto systémy neefektivní, protože potřebovaly tolik fyzických linek, kolik bylo potřeba vést souběžně telefonních hovorů. Z tohoto důvodu bylo vyvinuto částečně digitalizované řešení, kdy se na staré analogové telefonní rozvody s analogovými přístroji připojí digitálně řízená telefonní ústředna. Před tuto ústřednu se následně připojí hlasová brána a mezi ústřednou a sítí operátora probíhá komunikace skrze digitální protokoly. Při použití tohoto systému stačí pro komunikaci typem ústředny limitovaného počtu linek mezi ústřednou a operátorem pouze jediný pár vodičů. Při použití tohoto řešení organizace požádá o přidělení číselného rozsahu ze strany operátora, tyto linky jsou příslušnou technologií (ATM, BRI, ISDN, ADSL, aj.; popř. jejich kombinace přes převodníky) propojeny s ústřednou, která obsluhuje jejich mapování na vnitřní klapky. Výhodou tohoto řešení je, že je možné na jediné telefonní síti využívat hybridní systém, tzn. že využívá některé přístroje digitální, jenž jsou dražší, avšak nabízí rozšířenou funkcionalitu (identifikaci volajícího, popisky v rámci místních klapků, přepojování, hlasový záznamník, automatické přepojování při nepřítomnosti, atp.), pro koncové uživatele je však stále možné použít levnější analogové přístroje (často již v majetku z dřívější doby → finanční úspora). V dnešní době je však celé analogové řešení dávno zastaralé a plynule se přechází na VoIP. Rovněž je nutné zmínit fakt, že v případě vybavení budovy moderním systémem strukturované kabeláže je možné vyvázat výstupy z telefonní ústředny do racku a rozvést tak analogový telefonní rozvod právě touto strukturovanou kabeláží, což zároveň otevře cestu k likvidaci staré, často rozlámané a nevyhovující dvojlinkové kabeláže.

## **VoIP**

Nejmodernějším řešením místní telefonie je bez jakýchkoliv pochyb VoIP. Pod tímto akronymem se skrývají slova „Voice over IP“, kde IP je zkratka pro „Internet protocol“. Zjednodušeně řečeno se pod touto zkratkou skrývá volání přes internet. V realitě je však tento systém o mnoho složitější. Základním stavebním kamenem je pro VoIP telefony strukturovaná kabeláž pro připojení telefonů, dnes minimálně kategorie 5e pro zajištění komunikace v lokální síti o rychlosti 100 Mbps. VoIP telefony mají mnoho funkcí, které se liší podle řešení daného

výrobce. Obecně však nabízejí mnohem pokročilejší řešení telefonní sítě, než je tomu v případě sebelepšího analogového či hybridního řešení. Ta jsou totiž oproti VoIP často pouze jednoúčelová a nepočítá se u nich s jakýmkoliv dalším vývojem. Zásadními výhodami kteréhokoliv VoIP systému je modularita, škálovatelnost a nezávislost na aktuálně používaný set zařízení tvořící fyzickou topologii sítě.

Architektura typického VoIP systému spoléhá na standardní síť s fyzickou vrstvou zapojenou do hvězdy prostřednictvím kabeláže cat. 5e (nebo vyšší) sloužící jako trasa pro Ethernet rámce dle standardu 802.3u pro 100 Mbps, popř. 802.3ab pro 1000 Mbps, pro jednoduchost také často s využitím rozšíření 802.3af nebo 802.3at pro napájení prostřednictvím PoE (viz IP kamery).

Prostřednictvím této sítě využívající transportních protokolů TCP a UDP na síťové vrstvě IP si jednotlivé prvky VoIP systému vyměňují pakety, které obsahují data zapouzdřená dalšími protokoly. Tyto protokoly jsou jednak datové (obsahující hlasové vzorky), také však řídicí, prostřednictvím nichž je spravován na všech zúčastněných stranách celý přenos (nalezení spojení s protistranou, zjišťování její dostupnosti, jejích technických možností (kodek, přenosová rychlost, atp.), stavu (ready, vyzvánění, obsazeno, přesměrování, ...), atd. ). Zabíhat do popisu funkce jednotlivých protokolů je nad zamýšlený rozsah této práce. Hlavní pointou tohoto odstavce je, že kontrolních protokolů i kodeků se na trhu používá celá řada a který set je podporován v daném zařízení záleží výhradně na výrobcu daného zařízení či komplexního systému.

Každý VoIP systém sestává z několika hlavních součástí. Jak již bylo uvedeno výše, jsou to koncová zařízení (telefony), přenosová síť, dále se jedná o místní VoIP ústředny, popř. další specializovaná zařízení (VoIP brány, dveřníky, atp.).

### **Ústředny**

Srdcem každého VoIP systému je ústředna. Na rozdíl od starších časů, kdy se jednalo o velmi složitá zařízení, do kterých vedly desítky až stovky kabelů se v nejjednodušších případech jedná o malou krabičku s rozměry v jednotkách centimetrů, ve firemních aplikacích o zařízení podobné switchi do racku o velikosti 1-2 U. V nejnáročnějších případech se jedná o virtuální server, který může výpočetně pohánět cluster fyzických serverů. Poslední jmenované případy jsou však spíše případy telekomunikačních operátorů, než firemních zákazníků (a to i těch větších).

Oproti analogovým ústřednám můžeme zaregistrovat ještě jeden markantní rozdíl – do běžné VoIP ústředny vede jediný kabel a to datový. V náročnějších případech jich bude jen o pár více. Spojování v ústředně totiž neprobíhá formou spojování jednotlivých fyzických vodičů, ale formou datové komunikace a směrování datových toků. Vzhledem k faktu, že datová náročnost hlasových hovorů je i se standardními kodeky v porovnání s běžnými rychlostmi sítí naprosto mizivá (i s nejkvalitnějším kodekem G.711 se nedostaneme přes 100 kbps – pomalejší sítě dnes mají 100 Mbps), jeden kabel do ústředny tak postačuje svou propustností pro směrování několika set hovorů současně.<sup>18</sup> Limit maximálního počtu hovorů má tak, spíše než z důvodu omezení sítí, komerční charakter, popř. je tento limit dán výpočetní kapacitou ústředny – to je však, vzhledem k cenám ústředen, hardwaru v nich použitých a možnostem na trhu, velmi diskutabilní. Platí se tedy primárně za know-how daného výrobce.

VoIP ústředny se liší např. svou kapacitou (kolik SIP účtů zvládnou obsloužit), maximálním počtem simultánních hovorů, nabídkou funkcí, výpočetním výkonem nebo potenciálem pro rozšiřování skrze přídatné moduly (propojení s analogovou sítí, zálohování linky přes GSM, ad.).

Ze standardních funkcí společných pro většinu ústředen je možné jmenovat např.:

- zobrazování identity volajícího
- záznamník zmeškaných hovorů
- centrální registr hovorů (kdo, kam, jak dlouho, za kolik)
- manuální přepojování
- podmíněné přesměrování (v nedostupnosti spoj na sekretariát)

Za doplňkové funkce nabízené ústřednami můžeme uvést třeba:

- vytáčení přes webové rozhraní (zkopíruji číslo z webu a rovnou jej vytočím)
- centrální správa telefonního seznamu a jeho synchronizace s adresářem identit (XML, AD / LDAP)
- IVR – víceúrovňová automatická spojovatelka

---

18 Voice Over IP - Per Call Bandwidth Consumption. Cisco.com [online]. 2016 [cit. 2017-04-06]. Dostupné z: <http://www.cisco.com/c/en/us/support/docs/voice/voice-quality/7934-bwidth-consume.html>

- provisioning – autokonfigurace telefonního přístroje po zapojení do sítě
- fax-to-mail – převod faxů do e-mailu
- mail-to-SMS – přeposlání e-mailu SMSkou
- alert system – notifikace při aktivaci přednastavené události

Ústředny se obvykle připojí do veřejné telefonní sítě prostřednictvím rozvodu telekomunikačního operátora skrze tzv. SIP trunk, což je zjednodušeně virtuální sada telefonních linek vedoucí po Internetu do datacentra operátora. Odtud se náš hovor spojuje do veřejných telefonních sítí všude, kam si potřebujeme zavolat. Výhodou tohoto řešení je primárně cenová náročnost, využití již existující datové infrastruktury a neomezený potenciál pro rozšiřování systému v budoucnosti.

### ***Telefonní terminály***

V nabídce telefonních přístrojů pro VoIP je možné nalézt tři hlavní vývojové větve. Jsou to jednak klasické stolní telefonní přístroje připojované kabelem do rozvodů strukturované kabeláže. Tyto přístroje se vyznačují buďto nízkou cenou, případně vysokou funkcionalitou. Standardem u téměř všech přístrojů je dnes procházení centrálně spravovaného telefonního seznamu, přepojování nebo přesměrování hovorů v případě nedostupnosti. High-end přístroje pak mohou disponovat kvalitním LCD displejem s grafickým rozhraním, širokou paletou tlačítek pro rychlou volbu, propojením s cloudovými službami, popř. sadou nástrojů pro videohovory. VoIP je v tomto vysoce flexibilní a záleží jen na výrobci, zda ze svého zařízení udělá pouhý telefon nebo švýcarský nůž pro obsluhu různých systémů v korporátním komplexu. Zbývajících dvěma typy VoIP telefonů jsou bezdrátové telefony, označované také jako „handhelds“ nebo „ručky“. Prvním typem jsou bezdrátové telefony pro použití s proprietární základnovou stanicí (DECT), druhým typem jsou telefony určené pro práci ve WiFi sítích (existují však i hybridní zařízení).

Standard DECT (Digital enhanced cordless telecommunications) definuje fyzickou vrstvu bezdrátového spoje, kterou využije přenosný přístroj pro spojení s fixní stanicí. Nedefinuje však interní funkcionalitu sítě, což jej činí na jednu stranu velmi univerzálním, na druhou složitým na orientaci na trhu z pohledu koncového zákazníka. Je možné jej implementovat jak

do telefonů, tak i do zařízení nesloužící k přímé telefonii – využívají jej tak např. baby-monitory, hands-free sady, bezdrátová sluchátka, bezdrátová relé, ad.<sup>19</sup>

Základnové stanice DECT telefonů mohou mít různé provedení, vždy se však bavíme o architektuře master – slave, kde master je základnová stanice a podřízené jednotky jsou klientské terminály, tj. bezdrátové telefony. DECT definuje pouze komunikaci mezi terminálem a základnovou stanicí, co tedy již neřeší je propojení základnové stanice do nadřazeného telefonního systému. Je tak možné setkat se jak s DECT sety výhradně pro analogové sítě, tak se zařízeními pouze pro VoIP sítě, některé sety umožňují dokonce vybrat si příslušnou základnovou stanici k danému telefonu, popř. mohou mít tyto základnové stanice možnost pro připojení k oběma systémům. Obecnost standardu a omezení standardizace pouze na rádiovou část zařízení tak otevřela dveře kreativité vývojářů a tvůrců hardwaru.

Nezákladnější systémy nabízí architekturu 1 vysílač ↔ 1 telefon. Jedná se o běžně komerčně dostupné sety, které lze koupit velmi levně, neumožní však uživateli využít různých pokročilých funkcí.

Pokročilejší systémy dokáží na jediný vysílač připojit více telefonů (většinou max. 5). Ty naleznou uplatnění hlavně ve sdílených kancelářích, kde pro více uživatelů postačuje pro připojení pouze jediná základna a není tak nutné tahat několikanásobně kabeláž pro připojení k páteřní telekomunikační síti. Pro každý telefon pak postačí levný nabíjecí stojánek bez složité elektroniky.

Nejpokročilejší jsou pak buňkové sítě, které umožňují připojení prakticky neomezeného množství telefonů na jediný vysílač (ovšem s maximálním limitem souběžných hovorů) a navíc jsou schopné zajistit mobilitu všech zařízení v rámci kampusu. Volající tak není vázán na umístění vysílače, který zprostředkovává komunikaci mezi ručním přístrojem a kabelovou infrastrukturou a může se volně pohybovat všude v rámci dosahu signálu. To však u probíhajícího hovoru platí pouze za podmínky, že v místě, kde má dojít k roamingu, se překrývají signály sousedících buněk. Příkladem buňkových řešení založených na DECT mohou být např. řešení Well RTX, Gigaset N720, Spectralink 7000, aj.

Ruční VoIP telefony založené na technologii WiFi naleznou uplatnění primárně tam, kde již existuje kvalitní bezdrátová infrastruktura, popř. je-li potřeba ji vybudovat i za jinými účely a není dostatek financí pro vybudování samostatné sítě. Tyto telefony komunikují přímo s přístupovými body, nevyžadují existenci vlastní základnové stanice a tudíž ani související

---

19 DECT. European Telecommunications Standards Institute [online]. 2017 [cit. 2017-04-13]. Dostupné z: <http://www.etsi.org/technologies-clusters/technologies/dect>



kabelové infrastruktury. Podmínkou však je, aby existující WiFi síť byla bezpečná, stabilní a dokázala garantovat konstantní šířku pásma a minimální zpoždění pro VoIP komunikaci, velmi vhodné je také podpora komunikačních protokolů linkové vrstvy pro roaming mezi přístupovými body, což vylučuje použití levných spotřebitelských zařízení. Je nutno sáhnout po enterprise-class AP renomovanějších výrobců, optimálně řízených prostřednictvím controlleru (nebo podobným řešením). Zřizovat WiFi síť čistě pro účely zřízení lokální mobilní telefonie je však značně neekonomické. Výhodou je, že stávající metalickou infrastrukturu není potřeba rozšiřovat kvůli budování nezávislé telefonní sítě, dále je možné umožnit připojení chytrých telefonů a eliminovat tak nákup dalších přístrojů, nevýhodou je, že za cenu zařízení, které je nutno koupit lze vybudovat i řádově spolehlivější systém.

Při konzultacích s odborníky z praxe (Joyce, SIDIT) nebylo autorovi řešení VoIP na fyzické vrstvě WiFi doporučováno. Se slovy „pokud máš čtvrt milionu na wifiny, tak to pojede“ se svorně shodli, že mnohem raději ve škole uvidí buňkový DECT systém Well RTX, jelikož je ve výsledku neekonomičtější při zachování potřebných funkcí. Srovnáme-li totiž buňková řešení založená na standardu DECT se zařízeními pro WiFi podle jejich definujících technických standardů, zjistíme, že DECT má oproti WiFi několik značných výhod. Jedná se např. o využití pásma vyhrazeného čistě pro tyto účely, z čehož vyplývá, že DECT se potýká v městském prostředí se značně nižším rušením, než je tomu v silně zarušeném pásmu 2,4 GHz, které mohou v okolí používat stovky zařízení, které si navzájem ovlivňují funkcionalitu i bez hlasových systémů. I v případě koexistence více hlasových systémů je rušení v DECT minimální, jelikož výraznější komunikace mezi základnou a mobilními stanicemi probíhá pouze při aktivním přenosu, tj. při hovoru – WiFi jsou oproti tomu rušeny i provozem stovek dalších zařízení (ve škole, kde autor práce pracuje, je přes den běžně připojeno 500-600 WiFi klientů v jediné budově). Tento vliv se rovněž projeví při větším zatížení bezdrátové sítě a to na zvýšených latencích, což je při použití UDP paketů pro přenos hlasových dat silně kontraproduktivní. Jednou z vlastností UDP komunikace je totiž nulová garance doručení a pokud již pakety do cíle dorazí, nemusí se tak stát v požadovaném pořadí. To řeší sice do jisté míry protokoly vyšších vrstev, výsledek však nikdy nebude takový jako v případě vícebuňkového DECT, které se s těmito problémy vůbec nepotýká. Posledním a asi nejdůležitějším faktorem hrajícím pro DECT je operační frekvence. Oproti mikrovlnným datovým systémům v pásmu WiFi, tj. 2,4 GHz ( $\lambda = 12,5$  cm), popř. 5 GHz ( $\lambda = 5,6$  cm) operují DECT zařízení na delších vlnách. V operačním pásmu 1880 – 1900 MHz je tak vlnová délka  $\lambda = 15,8$  cm. V těchto frekvenčních pásmech platí pravidlo, že delší vlna má lepší průchodnost v prostředí plném překážek, než-li vlna kratší. V gigahertzových pásmech se totiž rychle

přibližujeme situaci, kdy se vlna šíří pouze odrazem, komunikace na nižších frekvencích se tedy v prostoru šíří lépe.

Souhra všech poznatků v případě lokální telefonní mobility hovoří jednoznačně ve prospěch DECT oproti WiFi.

I přes všechny výhody DECT sítí je však v dnešní době neomezených tarifů zvážit, zda se škole raději nevyplatí pořízení klasických mobilních telefonů a vyjednání výhodných podmínek s operátorem. Jednak dnes již není neobvyklé, že rámcové smlouvy má s operátory uzavřený zřizovatel školy za velice výhodných podmínek a je tak možné např. dosáhnout stavu, kdy si všichni zaměstnanci převedou soukromá čísla pod tuto rámcovou smlouvu, budou za své soukromé hovory platit méně, zodpovídat za své faktury sami a v rámci VPN (všechny telefony pod smlouvou zřizovatele) si budou volat naprosto zdarma. Je však nutné vzít v potaz i fakt, že škola přichází o možnost přepojovat hovory, jednoduše centrálně spravovat telefonní seznam nebo volat do zahraničí za jednotky korun za minutu (byť se v tomto ohledu situace mění, autorovi není smlouva podobného ražení známa). Každý případ má své klady a zápory a v této oblasti nelze, s ohledem na výše uvedené důvody, doporučit jedno univerzální řešení.

### **2.1.3 Datové sítě**

#### **Metalické sítě**

Datová síť v budově ke nezbytnou prerekvizitou pro provoz dalších technologických celků, ať už se jedná o byt, dům, kancelář, velkou továrnu, malou vesnickou základní školu nebo třeba střední školu s mnoha budovami. Je zde možno kontraargumentovat, že malá škola přeci není na těchto systémech tak závislá, jako ta velká – a je to pravda. Z pohledu autora by se tato závislost však měla stát dnes v určitých ohledech nezbytnou nutností.

Vzhledem k rozvinutosti informační společnosti a tendencím v sektoru služeb i průmyslu snižovat náklady skrze automatizaci a z toho vyplývajícího poklesu poptávky po nekvalifikované pracovní síle lze s postupným nástupem konceptu Průmyslu 4.0 předpokládat, že do budoucna bude primární úlohou českého školství připravovat pro trh práce nikoliv žáky orientované na manuální dovednosti, avšak vysoce kvalifikované a úzce specializované odborníky, kteří budou muset i na nejnižších pomocných pozicích zvládnout práci s pokročilou výpočetní technikou. Lze tudíž předpokládat růst nároků na současné i budoucí žáky po stránce informační gramotnosti. Jelikož by škola měla připravovat žáky na situace, které je čekají v reálném životě, je vzhledem k tempu rozvoje informačních technologií více než nutné častěji modernizovat současné zastaralé vybavení škol. V současnosti panuje na školách trend vzdělávat žáky

prostřednictvím počítačových učeben se standardními PC vybavenými operačním systémem MS Windows (v různých verzích), kancelářským balíkem MS Office (v různých verzích) a jiným programovým vybavením. V současné době však můžeme zaznamenat i nový trend a to zařazování výuky prostřednictvím počítačů i do jinak striktně netechnických hodin (zeměpis, angličtina, dějepis, ...). Tato situace v mnoha školách zvýšila poptávku po počítačových učebnách natolik, že na v aplikační části zkoumané škole se nyní plánuje realizace již čtvrté počítačové učebny (cca. 700 žáků).

Rostoucí množství počítačů ve škole vzhledem k technickým řešením dnešního software a nárokům na správu přináší vysoké nároky na propustnost datových sítí. Jak již bylo uvedeno v kapitole o strukturované kabeláži, ty na to nejsou často vůbec připraveny. Jeví se tedy jako velice vhodné ze strany vedení školy alokovat ročně určitý objem financí za účelem obměny a modernizace technologií datových sítí a serverového zázemí. Z vlastní zkušenosti autora se totiž často stará síťová technologie vyměňuje až v momentě, kdy selže a celá škola je pak bez spojení se světem. V době, kdy většina práce účetních spočívá v práci s portály státní správy a kdy učitelé běžně pracují s digitálními učebními materiály není oč stát.

Jako optimální stav se jeví situace, kdy škola disponuje vysokorychlostním připojením do Internetu prostřednictvím optické linky, vysokorychlostní LAN (optimálně 1 Gbps plošně a 10 Gbps na páteřních trasách) zajištěnou managovatelnými switchi, má k dispozici vlastní kvalitní plně virtualizovanou serverovou infrastrukturu, rychlá disková pole s disky v RAID 10, sekundární server v jiné části budovy pro ukládání záloh a replikaci doménového řadiče, e-mailů hostované v rámci cloudového řešení (např. GSuite for Education) a všechny počítače v síti disponují jednotným obrazem nejnovějšího systému, jsou zařazeny do domény a jsou vybaveny centrálním antivirovým řešením a softwarem pro dálkovou správu (např. Comodo ONE MSP). Popsané řešení je však na hony vzdálené od reality a to kvůli limitovaným finančním možnostem škol.

Lze se tak v praxi setkat se sítěmi, které padají cca. třikrát za hodinu jen proto, že použité switche nejsou vybaveny moderní funkcionalitou, která dokáže např. vytvořit virtuální logické síť a oddělit tak provoz v jednotlivých segmentech (broadcast doménách), což vede ke snižování zátěže aktivních prvků (prohledávání kratších MAC tabulek). Častým jevem je také přítomnost jevů označovaných jako „bottleneck“, což v překladu znamená hrdlo lahve. Jedná se o situaci, kdy klienti v rámci jednoho segmentu sítě jsou schopni komunikovat velmi rychle a efektivně, avšak pro propojení mezi segmenty je použita linka s nedostačující kapacitou. Tento problém si lze jednoduše vizualizovat. Představme si 10 počítačů snažících se současně získat 100MB

soubor ze serveru v druhém segmentu sítě. Každý počítač je do sítě připojen 100Mbit linkou, segmenty jsou však mezi sebou rovněž propojeny jedinou 100Mbit linkou. Veškerý provoz mezi těmito segmenty je tak limitován nejpomalejším článkem řetězu. Maximální rychlost přenosu tak bude v optimálním případě 10 Mbit pro každý počítač, reálně spíše o pár procent méně (overhead). Připočteme-li k této zátěži i nefiltrovaný broadcast storm a často i výkonově poddimenzovaný směrovač, máme problém – síť nefunguje pořádně nikomu. S tímto jevem je nejčastěji možné se ve škole setkat při dodatečném rozšiřování počítačových učeben o další PC, kdy na tyto změny nejsou dimenzovány současné datové rozvody v učebně. Často si tak zodpovědní pracovníci ulehčují práci a na přírodní 100Mbps linku původně pro jediný počítač napojí třeba 7 nových.

Z výše uvedených důvodů se jako nejvhodnější řešení jeví využití optických páteřních spojů (optimálně SM 9/125), jelikož optické vlákno není, na rozdíl od metalické kabeláže, limitováno maximální možnou operační frekvencí (v dnešních limitech) a má tak do budoucna mnohem větší potenciál pro rozvoj (např. lze v budoucnu využít multiplexory a propustnost tak znásobit). Při využití switchů se sloty pro moduly SFP je možné využít maximální rychlosti 1,25 Gbps, pro moduly SFP+ je pak maximum 10 Gbps. Ve školách je dnes 10 Gbps vysoce moderní standard, na trhu lze však nalézt i moduly pro sloty QSFP+ s maximální rychlostí 40 Gbps a dokonce i libůstku v podobě CFP modulů nabízející maximální rychlost 100 Gbps. Na zlevnění nebo levnější náhradu posledně jmenovaných technologií si však budeme muset ještě pár let počkat. Rychlost páteřního spoje by měla být v dostupné řadě minimálně o řadu vyšší, než rychlost připojených klientů. Pro klienty na 100Mbps síti je tak vhodné využít páteřní spoje o rychlosti 1 Gbps, využijeme-li pro klienty gigabitového připojení, páteřní síť by měla mít rychlosti minimálně 10 Gbps, atp. Máme tak garanci, že i pokud pojedou 10 klientů na plný výkon (což je prakticky nereálné), síť tyto přenosy zvládne kapacitně obsloužit.

Datová síť hraje velice důležitou roli i v případě jejího využití jako přenosového média pro VoIP telefony, kamery nebo streamovaná multimédia. Taková síť totiž musí být vysoce spolehlivá a optimálně by měla provozovat každou tuto aplikaci na samostatné vyhrazené virtuální síti s garantovanou šířkou pásma. Je proto nutné síť dostatečně nadimenzovat jak kapacitně, tak i výkonově (přepínací a směrovací výkon), aby nedocházelo k zahlcení jak linek, tak výpočetních jednotek aktivních prvků.

Datové sítě ve školách se dnes stávají vysoce komplexní záležitostí, kterou většinou nejsou efektivně schopni spravovat lidé věnující se primárně pedagogické činnosti. Častou chybou, se kterou se autor setkává v praxi, je tudíž vedením iniciované a úsporami motivované

svalení zodpovědnosti za tyto technologie na učitele informatiky, techniky, popř. jiných přírodních věd. Z pohledu bezpečnosti je však toto řešení potenciálním rizikem (a ne zrovna malým), a to primárně proto, že člověk věnující se na plný úvazek pedagogické činnosti se nedostane do denního kontaktu s technickými problémy, není obvykle v této specifické oblasti průběžně vzděláván, nestíhá průběžně sledovat vývoj na trhu nemůže tak prediktivně uvažovat při nastavování bezpečnostních politik v organizaci. Ve výsledku tak může škola kvůli šetření na nesprávném místě paradoxně hodně prodělat. Často totiž tento princip funguje na bázi „co zvládneme, to si uděláme sami a co ne, necháme na firmě“. Firmy se tohoto naučily využívat a jednorázové zásahy do sítě, kterou ve výsledku spravuje více lidí, tak leckdy nakonec vyjdou školy draž, než kdyby se o ni starala výhradně externí organizace s využitím svých standardizovaných metodik, postupů a preventivních opatření vycházejících ze zkušeností získávaných i z jiných spravovaných lokalit.

## **Bezdrátové sítě**

Když mezi lidmi pohybujícími se ve sféře školního IT nadnesete téma „školní wifi“, dočkáte se obvykle nekončícího přívalu argumentů, na které nebude pravděpodobně nikdy existovat jednoznačná odpověď, která by uspokojila všechny zúčastněné. Mají ve školách co pohledávat bezdrátové sítě? Je „wifina“ opravdu tak potřebná?

Názor autora na tuto problematiku je takový, že bezdrátová datová síť by měla být standardem v každé škole. Ať už na škole základní nebo střední. Autor rovněž klade důraz na dodržování síťové bezpečnosti a podporuje i stanovení a vynucení interních pravidel pro jejich provoz.

Bezdrátové datové sítě, se kterými se dnes můžeme běžně setkat jsou definovány standardem IEEE 802.11 (+ příslušným písmenem). Tento set standardů různého stáří definuje nejčastěji fyzickou a část linkové vrstvy (případně šifrování, dále také roamingové technologie, apod.) bezdrátových sítí známých veřejnosti spíše jako „wifi“. V běžně používaném režimu sítě, tj. v režimu infrastruktury, funguje síť topologicky hvězdicovitě. Středem hvězdy však není metalický switch, avšak tzv. „access point“, zkr. AP, v překladu přístupový bod.

Zde pokládá autor za velmi nutné zdůraznit rozdíl mezi AP a wifi routerem. AP komunikuje s bezdrátovými klienty stejným způsobem jako wifi router, avšak wifi routery jsou zařízení kombinovaná, sloužící primárně k oddělení segmentů sítě, nejčastěji vnější sítě poskytovatele internetových služeb od sítě vnitřní (zákazníka). Typický AP mívá pouze jediný

konektor pro připojení páteří metalické sítě, wifi router jich mívá více, přičemž jeden je obvykle vyhrazen právě pro vnější metalickou síť. Tato zařízení jsou určena hlavně pro domácnosti a malé kanceláře, nikoliv pro komplexní školní budovy. Rozdíl v logice fungování těchto dvou zařízení je markantní – wifi router routuje (směruje) pakety na třetí vrstvě modelu ISO/OSI, zatímco AP je pouze brána do existující metalické infrastruktury a obecně se zabývá pouze vrstvou L2.

Bezdrátové sítě mohou mít různorodé určení. V praxi sice slouží nejčastěji k připojení mobilních zařízení do sítě Internet, obecně však slouží k přenosu datových paketů mezi dvěma body (neuvažujeme nyní Ad-Hoc sítě). Nelze proto jejich funkcionalitu zužovat pouze na připojení do internetu. Jak již bylo popsáno v kapitole 3.1.2 při rozboru VoIP telefonie, lze jejich prostřednictvím i telefonovat, z dalších aplikací lze vyjmenovat např. bezdrátový tisk, streamování na informační TV bez nutnosti tahat nové datové linky, spojení meteostanice se serverem či připojení tabletů pro práci s mobilní verzí školního informačního systému.

Podívejme se zpět na problém řešený na počátku, tj. kdo by měl mít k takové síti přístup. Autor zastává názor, že ať už se jedná o kteroukoliv školu, měli by k síti mít přístup všichni zaměstnanci, ať už pedagogové nebo nepedagogičtí zaměstnanci. Při možnostech dnešní techniky rozhodně není problém připojit těch několik málo lidí (na velkých školách do stovky jedinců, reálně toho však stejně všichni nevyužijí). Zaměstnanci by měli mít k dispozici vlastní síť (SSID) s kvalitním šifrováním (WPA2-AES) a optimálně i ověřováním identity vůči RADIUS serveru. Tuto síť je vhodné oddělit od sítě používané pro technické účely (výše jmenované meteostanice, tiskárny, telefony, TV, atp...).

Nyní si rozeberme otázku, zda je vhodné pouštět k wifi žáky. Jelikož se touto problematikou autor aktivně zabývá, setkal se během své praxe s různými protichůdnými názory. V jednom bodě však převládá obecná shoda – na základních školách to rozhodně nemá smysl a bylo by to pouze ke škodě žáků. Co se však středního školství týče, zde již tak obecná shoda nepanuje. Obecně se jedná o konflikt dvou názorových proudů:

- WiFi pro žáky SŠ je vhodným nástrojem pro žáky i učitele, z jehož využívání mohou, pokud je v hodinách využít správným způsobem, prospívat obě strany.
- WiFi pro žáky SŠ není vhodné zavádět, protože pak žáci nedávají pozor v hodinách a nezvládají učební látku.

Autor zavádění volně přístupných wifi sítí pro žáky středních škol podporuje. Prvním důvodem je, že druhý z uvedených názorů je nejčastěji možné slyšet z úst vyhořelých pedagogů, kteří si

dle hodnocení nadřazených rádi ulehčují práci, odmítají se učit nové věci a přístupy a neumí dobře pracovat se skupinou žáků. Druhým důvodem je již výše rozebíraná úloha školy, která má žáky připravovat na budoucí život, kam tyto technologie jednoznačně patří a žáky rozvíjet, nikoliv je v rozvoji omezovat. Vždy je na učiteli, jakým způsobem si nastaví pravidla hodiny, navíc střední škola není pro žáky povinná a kdo se učit nechce se s velkou pravděpodobností stejně učit nebude, ať už má k dispozici wifi nebo ne.

Markantnějším problémem při zavádění těchto systémů do školy jsou již tradičně finance. Na trhu je široké zastoupení výrobců, kteří skrze své distributory nabízejí různá technická řešení pro wifi, kdy každé řešení nabízí trochu jiné funkce. Základním požadavkem na AP pro školní síť by měla být rozhodně možnost centralizované administrace systému na jediném místě. Už jen tento požadavek vylučuje z možností veškeré wifi zařízení běžně dostupné v obchodních řetězcích, třebaže i v těch zaměřených na elektroniku. Za účelem nákupu podobných zařízení je velmi vhodné udělat si vlastní důkladný průzkum trhu, následně přímo oslovit distributory (nikoliv koncové prodejce) jednotlivých značek, projednat požadavky své školy s ohledem na možnosti rozšiřování i do budoucna, věnovat celému projektu potřebný čas (klidně i půl roku) a následně vybrat zařízení, která se budou schopna vypořádat s nároky na řízení celé sítě, ať už jde o mechanismy pro férové řízení datového toku, filtry obsahu (důležité např. pro omezení kyberšikany), mechanismy pro rozkládání zátěže mezi jednotlivé AP, mechanismy pro ověřování, šifrování nebo např. o potřebu koupě separátního kontroleru (který celé řešení zbytečně prodraží), nutnost licencovat operační systém AP podle jejich počtu v síti nebo třeba maximální počet klientů na AP a jejich výpočetní výkon. Autor práce využívá v praxi při tvorbě řešení s vysokou koncentrací uživatelů technické řešení HPC Aruba iAP, kde jeden kus iAP-103 stojí cca 6500,- Kč s DPH, systém funguje v režimu multi-master bez potřeby kontroleru, ten je však možné dokoupit a rozšířit tak funkcionalitu systému. Systém zvládá dle zkušeností autora při správném nastavení spolehlivě obsloužit i 80 uživatelů na každém AP, je odolný proti výpadkům všech ostatních AP a disponuje několika kvalitními ochrannými mechanismy. Pro méně náročné aplikace pak autor doporučuje využít řešení firmy Ubiquiti Networks a to konkrétně zařízení Unifi AP AC LR v kombinaci se zařízením Unifi Cloud Key, který umožňuje systém ovládat vzdáleně přes veřejné cloudové rozhraní poskytované výrobcem v režimu SaaS<sup>20</sup>. Obě řešení se autorovi osvědčila při několika aplikacích (střední škola se sedmi sty žáky, internát, rekreační středisko, 2 hotely).

---

20 What is SaaS? Interoute.com [online]. 2017 [cit. 2017-04-06]. Dostupné z: <http://www.interoute.com/what-saas>

## Počítače

Stáří počítačů není obvykle věc, kterou by se české školy mohly chlubit. Počítače jsou však prvkem, s nímž uživatelé denně pracují a tudíž tím, co z jejich pohledu ICT tvoří. Jejich kvalita, nastavení, softwarová výbava a spolehlivost jsou tak hodně důležité proměnné, o které by mělo být dbáno, ICT ve školách je primárně pro usnadnění práce lidem. Jelikož však školy často nemají finance na zakoupení nových výkonných strojů, je možné se často setkat s rozhodnutím „koupíme nové, až budou peníze“.

Problémem je však stárnutí elektroniky a prakticky okamžitá ztráta její hodnoty po zakoupení. Nové počítače jednak stárnou ze dne na den, nové rovněž neznamena vždy nutně kvalitní. Jednak je poruchovost nových výrobků vyšší, než poruchovost výrobků používaných, viz vanová křivka<sup>21</sup>, leckdy je také kvalitnější věc starší, avšak původně řádově dražší. Původně dražší a kvalitnější věci mohou mít křivku četnosti poruch posunutou o notný kus níže, než zařízení levná a nová. Do škol je tak např. možné za zlomek původní ceny zakoupit vyřazené pracovní stanice 3D vývojářů, které již v současnosti nesplňují softwarové nároky pro využití nejmodernějších programů využívaných v komerčním sektoru. Za cenu těchto starších špičkových výrobků bychom dnes stěží koupili sestavu, která by jí byla schopna konkurovat po stránce výkonu i kvality zpracování (a tudíž i životnosti). Obrovskou výhodou školství oproti komerčnímu sektoru jsou nízké nároky na výkon výpočetní techniky, pro běžnou práci tak postačují zařízení z roku 2008 a výše. Pro řádové navýšení výkonu se pak (s přihlédnutím k padajícím cenám) přímo nabízí možnost výměny poruchových a pomalých mechanických pevných disků za elektronické SSD, což např. při velikosti 120 GB vyjde na 1700 Kč včetně DPH za nový disk s tříletou zárukou<sup>22</sup> a životností, dle recenzí srovnatelné technologie z roku 2015<sup>23</sup>, přesahující životnost dvou počítačů. Kapacita 120 GB bohatě stačí pro počítače určené pro třídy, nedostatek kapacity (např. na PC v kabinetech) lze řešit buď dokoupením přídatného disku, v lepším případě však připojením síťového úložiště skrze souborový server. Pro takové úložiště je pak velmi jednoduché nastavit automatické zálohování, ať už formou živé replikace disků (RAID / Storage Spaces) nebo verzovaným zálohováním.

Školám ve zvláště tíživé finanční situaci lze pak doporučit navázání spolupráce s komerčním sektorem, kde je zvykem výpočetní techniku v pravidelných intervalech

---

21 VDOLEČEK, František. Spolehlivost a technická diagnostika [online]. Brno: VUT v Brně - Fakulta strojního inženýrství - Ústav automatizace a informatiky, 2002, s. 8-9 [cit. 2017-04-06]. Dostupné z: <http://autnt.fme.vutbr.cz/lab/a1-731a/FSD.pdf>

22 Patriot Flare 120GB - Srovnání cen. Heureka.cz [online]. 2017 [cit. 2017-04-06]. Dostupné z: [https://pevne-disky.heureka.cz/patriot-flare-120gb-2\\_5-sata-ssd-pf120gs25ssdr/](https://pevne-disky.heureka.cz/patriot-flare-120gb-2_5-sata-ssd-pf120gs25ssdr/)

23 OCZ Vector 150: v testu výdrže jej umučíme k smrti. Svethardware.cz [online]. Brno, 2015 [cit. 2017-04-06]. Dostupné z: <http://www.svethardware.cz/recenze-ocz-vector-150-v-testu-vydrze-jej-umucime-k-smrti/40050>



obměňovat. Místo cesty na sběrný dvůr tak může vyřazená technika sloužit ještě nějakou dobu ve školách, kterým může např. pomoci překlenout období, než bude alokován příslušný rozpočet na pořízení vlastní, potenciálně lepší techniky. Podobně může být tato spolupráce navázána s ostatními školami v regionu, případně jinými institucemi zřizovatele. Co jedné organizaci již nevyhovuje může stále parametricky vyhovovat organizaci jiné.

### **3 Bezpečnostní a dohledové systémy**

V ČR pravděpodobně neexistuje škola, která by ve svých prostorech nikdy neřešila krádež majetku, osobních věcí žáků nebo zaměstnanců nebo vniknutí neoprávněných osob do různých prostor. Majoritním důvodem je fakt, že každá škola je z povahy instituce veřejně přístupným zařízením s velmi obtížně kontrolovatelným pohybem osob – vždyť areály školy leckdy slouží jako park, tělocvičny se pronajímají zájemcům z řad veřejnosti, v zařízeních odborného výcviku se veřejnost leckdy pohybuje cíleně (školní autoservis, kadeřnictví, zahradnictví, ...) nebo se přímo ve škole odehrávají různé kulturní či společenské akce. I tradiční třídní schůzky dávají příležitost k nepozorovanému vniknutí osob s nekalými zájmy a to ještě nedošlo na zmínku potenciálního pomstychtivého chování ze strany problémových žáků, ať už jsou příčiny jakékoliv. To vše přináší zvýšené nároky z hlediska zajištění bezpečnosti žáků a zaměstnanců školy, majetku a v neposlední řadě také informací uložených v těchto prostorech. Jelikož doba pokročila a k hlídání a dozoru není nutné využívat služeb vrátných, nočních hlídačů a psů, budou následující řádky věnovány popisu systémů sloužících k prevenci i represí nezákonného jednání na půdě školy.

#### **3.1 Elektronické zabezpečovací systémy**

Tyto systémy jsou známé spíše pod zkratkou „EZS“, lidověji se označují výrazem „alarm“ (přejato z angličtiny, v překladu upozornění / výstraha). EZS se za dobu své existence dostaly již do rozsáhlé většiny budov, i když třeba pouze částečně. Školy nejsou výjimkou. Primárním účelem je ochrana nemovitého majetku před neoprávněným vniknutím, movitého majetku před zcizením, popř. ochrana osob v nouzových situacích či před ohrožujícími environmentálními vlivy.

Ve školství se tyto systémy uplatní zejména při ochraně průchozích a přístupových prostor (chodby, schodiště, vchody), při ochraně prostor s vyšší kumulací dražšího majetku.

Každý EZS sestává z několika základních subsystémů, které budou detailně rozebrány v následujících podkapitolách:

- detekce
- ovládání
- analýza
- komunikace
- (volitelně) řízení programovatelných výstupů – v moderních EZS již standard – viz níže

Následující řádky vycházejí hlavně z praxe autora, popř. z konzultací s technickou podporou jednak českého výrobce Jablotron, jednak také distributora produktů kanadské společnosti Paradox security systems do ČR, společnosti Variant Plus v Třebíči.

### **3.1.1 Detekce**

Pro účely získávání vstupních hodnot využívá EZS tzv. detektorů. To jsou zařízení, která aktivně či pasivně vyhodnocují různé fyzikální parametry v daném prostředí a slouží nám tak ke sběru vstupních dat pro vyhodnocovací logiku ústředny. Základem detektoru je napájení, samotné čidlo, pomocná a logická elektronika a výstupní médium (svorkovnice / rádiový komunikátor).

#### **Obecné dělení detektorů**

Rozlišujeme detektory:

- stavové
  - jsou schopny informovat o změně stavu na detektoru, např. magnetický detektor je schopen zaslat ústředně zprávu, že je otevřen nebo uzavřen
- pulsní
  - pulsní detektor není schopen ústředně hlásit uklidnění, tento typ detektorů zasílá informaci pouze v případě, že registruje poplachovou hodnotu (např. pohyb), následné zpracování uklidnění je řešeno vypršením časového intervalu, popř. složitějším logickým zpracováním (potvrzování poplachu, atp.)

- datové
  - tyto detektory zasílají ústředně proměnné datové hodnoty, může se jednat např. o detektory teploty, spotřeby, čítače pulzů, detektory s kamerou, atp.

Také lze využít dělení podle způsobu komunikace, a to na:

- drátové standardní (pro přímé zapojení do hvězdicové topologie ústředny)
  - s NC kontaktem (NC = normally closed – v klidu je kontakt sepnut)
  - s NO kontaktem (NO = normally open – v klidu je kontakt rozepnut)
- drátové sběrníkové
- bezdrátové

Každý detektor musí být bezpečný, za běžného provozu systému neodpojitelný a v případě ztráty komunikace s detektorem musí být ústřednou vyhlášen poplach. Proto se využívá tzv. tamper kontaktů (z anglického slovesa „tamper“ = zasáhnout do funkce), což jsou spínače, které jsou rozpojeny v případě otevření krytu detektoru nebo jeho stržení detektoru z instalační pozice. U sběrníkových a bezdrátových detektorů je snímání a předávání informací z tohoto kontaktu řešeno přímo elektronickými obvody detektoru. Jen u standardních drátových detektorů je tento kontakt vyveden na svorkovnici, na které je zapojení detektoru voleno instalačním technikem dle možností připojované ústředny a požadavků na bezpečnost. Lze se setkat se zapojeními s vyvažovacími odpory nebo bez, popř. v ATZ módu (2 hodnoty vyvažovacích odporů pro rozlišení sepnutí dané zóny). Výhodou přímo připojovaných detektorů je, že v případě přestřižení přívodního kabelu potenciálním lupičem dojde na ústředně k okamžité změně hodnoty odporu mezi svorkami daného detektoru, na což ústředna briskně reaguje, zatím co u sběrníkových systémů je výpadek komunikace ústředny s detektorem zaznamenán až po několika neúspěšných pokusech, čili je zde potenciální prostor pro krátkodobé vyřazení detektoru z provozu. U bezdrátových zařízení je možné na krátký čas cíleně zarušit komunikační pásmo a vyřadit tak detektory z provozu, avšak toto je již jev ústřednou detekovatelný.

A nakonec můžeme detektory dělit také na:

- pohybové
- plášťové
- environmentální

## **Pohybové detektory**

Pohybové detektory jsou nejčastěji využívaným typem. Zaznamenávají pohyb v pokrývaném prostoru a informují o tomto dění ústřednu. Pohybové detektory existují v mnoha různých provedeních, které se liší primárně úhlem, velikostí plochy a tvarem snímaného prostoru, dále se mohou lišit i použitou technologií, citlivostí (odolností vůči falešným poplachům) a možnostmi nastavení detekce.

Základním typem pohybových detektorů jsou tzv. PIR detektory. Za zkratkou PIR se ukrývá sousloví „passive infrared“, kde infrared se v technické angličtině běžně zkracuje jako IR (stejně jako UV v případě ultrafialového záření (ultraviolet)). Pro vysvětlení základních principů fungování PIR detektorů si dovoluji odcitovat vybrané části vynikajícího naučného článku z portálu pro vývojáře elektroniky hw.cz:

*„Čidlo funguje na principu pyroelektrického jevu. [...] Podobně jako mechanickým tlakem lze deformovat krystalickou mřížku dielektrik, můžeme tuto deformaci vyvolat i změnou teploty. V látkách s jednou polární osou symetrie tak lze změnou teploty vytvářet dipólový moment, jehož velikost je přímo úměrná změně teploty a má směr této polární osy symetrie. Tento jev byl znám již od 17. století z pozorování přitahování částic popela k jednomu konci chladnoucího krystalku turmalínu, nalézaného v přírodě (Ceylon). Podle řeckého slova pyros = oheň byl jev nazýván jevem pyroelektrickým. Obecně lze pyroelektrický jev definovat jako schopnost materiálu generovat dočasný elektrický potenciál při změně jeho teploty.*

## **PIR Element**

*Pyroelement je polovodičová součástka (ze sloučenin na bázi lithia a tantalu). Pyroelektrické detektory jsou citlivé na ozáření infračerveným světlem tak, že začnou generovat elektrický povrchový náboj Q. Pokud se změní hodnota dopadajícího infračerveného záření na povrch pyroelektrického materiálu, změní se tím i hodnota elektrického povrchového náboje. Tato změna*

*náboje je měřena citlivým FET tranzistorem, který je přímo vestavěný ve snímači. Pyroelektrický snímač je citlivý ve velkém vlnovém rozsahu a proto je před pyroelektrický snímač aplikován filtr záření, který propouští infračervené záření o vlnových délkách v rozsahu 8 až 14  $\mu\text{m}$ . Lidské tělo emituje do prostoru záření o vlnové délce 9,4  $\mu\text{m}$ .“<sup>24</sup>*

Článek je mnohem delší a obsahuje velký objem technických podrobností, které však silně přesahují zamýšlený rozsah této práce, po podrobnostech prahnoucí čtenář necht' proto navštíví zdroj.

Shrme a rozšíříme si uvedené poznatky: PIR detektory snímají infračervené pozadí prostoru, kde pracují. Pohyb osob mohou zaznamenat proto, že lidé vyzařují díky vlastnímu metabolismu infračervené záření, které kontrastuje se studeným pozadím objektu. PIR detektory obsahují pyroelementy, které se nacházejí za čočkou směřující na ně záření z hlídaného prostoru a reagují na změnu toku dopadajícího infračerveného záření změnou elektrického potenciálu mezi kontakty. Vzniklé napětí je snímáno vyhodnocovací elektronikou, která zároveň eliminuje nastavitelnou logikou falešné poplachu a v případě pozitivní detekce předává, v závislosti na použitém rozhraní, informaci ústředně. Výraznou nevýhodou PIR detektorů je, že v případě, že nejsou vybaveny antimaskingem, lze je snadno obelstít – jednoduše je lze zalepit. I takto ošetřená čidla se však dají s troškou umění pomalu obejít s velkým černým deštníkem, který má stejnou teplotu jako okolí a zastíní tak detektoru záření emitované člověkem, popř. lze místnost vzdáleně přetopit na tělesnou teplotu za účelem zrušení tepelného kontrastu pozadí. Další nevýhoda těchto detektorů spočívá v nízké odolnosti proti falešným poplachům – detektory reagují na infračervené záření, které může vydávat prakticky cokoliv. Stačí, aby v zorném poli detektoru byl zdroj tepla. Kvalitní detektory si s valnou většinou běžných situací dobře poradí, avšak těm horším stačí ke spuštění poplachu automaticky sepnuté topení, lednička, silněji se zahřívající počítač nebo odlesk slunce od skleněného stolu. Lze se setkat také s čidly, která nejsou schopna zareagovat ani tehdy, když mají. Výrobci proto využívají různých metod, jak se s těmito problémy vypořádat.

Jednou z metod je využití kvalitních IR filtrů, které propustí užší spektrum záření specifické pouze pro člověka. Levné filtry mohou propouštět i jiné části spektra, načež sebekvalitnější pyroelement zareaguje falešným poplachem.

Další metoda je nasazení propracované digitální analýzy signálu, která dle výše citovaného článku, oproti analogové analýze počítající pouze četnost reakcí přes prahovou

---

<sup>24</sup> PIR detektor: skvělý sluha, ale zlý pán. Vyvoj.hw.cz: Profesionální elektronika [online]. 2013 [cit. 2017-04-06]. Dostupné z: <http://vyvoj.hw.cz/automatizace/pir-cidlo-skvely-sluha-ale-zly-pan.html>

hodnotu, zkoumá krom amplitudy signálu „i jeho strmost, polaritu, časování, povahu energie a kmitočtové spektrum společně se statistickými informacemi, které byly zjištěny průzkumem prostředí“. Pro analýzu je u kvalitnějších výrobků možné v detektoru nastavit i různé stupně citlivosti, čímž lze např. eliminovat vyhlášení poplachu při proběhnutí drobného zvířete (z vlastní zkušenosti autora např. myš v dílně, nebo pavouk prolézající před detektorem).

Zvláštní kapitolu představují PIR pro venkovní použití, které se od těch klasických pro vnitřní použití liší jednak materiálem použitým pro výrobu obalu, jednak ale také filtry vlnových délek konstruovanými tak, aby co nejlépe utlumily vliv slunečního záření a přitom propustily co nejužší spektrum záření vyzářovaného lidským metabolismem.

Jedním z problémů, který se nevyskytuje ani tak u instalací ve veřejných prostorech, jako spíše v domácích, je požadavek na zajištění objektu s tolerancí přítomnosti psa nebo kočky v objektu. Za tímto účelem se využívá několika technologií. Buď lze využít výměnných čoček, které na pyroelement nesměřují záření z oblastí při zemi (např. snímají pouze oblast nad 1 m), popř. lze využít dvousnímačových detektorů, kde jeden pyroelement snímá oblast při zemi, druhá nepřekrývající se oblast nad tou první. Pro vyhlášení poplachu je pak potřeba logický součin (AND), tzn. že dokud nevyhlásí poplach obě části detektoru současně, celý detektor zůstává v klidovém stavu.

Na sadě obrázků v příloze 1 je možné porovnat různé tvary a snímací charakteristiky PIR detektorů (nástěnný jednozónový s chodbovou, zvířecí a záclonovou čočkou, stropní detektor, vnitřní dvouzónový, venkovní ).

Chytrou metodou jak zabránit jak obelstění PIR detektorů, tak falešné poplachy je jejich kombinace s nízko-výkonovými mikrovlnnými radary. Jeden detektor tak obsahuje jak PIR modul, tak mikrovlnný modul. MW modul měří odrazivost mikrovln o frekvenci 9,35 GHz ( $\lambda = 3,2$  cm), která se v klidném prostoru skokově nemění). Této kombinace detektorů můžeme využít ve dvou variantách. Pro zvýšení bezpečnosti je možné využít logického součtu (OR), kdy pro vyhlášení poplachu na detektoru postačí poplach na jediném čidle ze dvou. Pro zvýšení odolnosti proti falešným poplachům je pak možno využít již popisovaného logického součinu (AND).

## **Magnetické detektory**

Ponecháme-li stranou detektory sloužící k monitorování pohybu v prostoru, dalším nejčastěji využívaným typem jsou detektory magnetické sloužící k hlídání odchylek pohybu zařízení

s danou dráhou pohybu od normálního stavu. Slouží nejčastěji k hlídání dveří, oken, avšak je s klidem možné je využít k hlídání stavu garážových vrat, posuvných bran, šatních skříněk, stmívacích rolet nebo třeba jen servisních dvířek u uzávěrů plynu či vody.

Magnetické snímače jsou principem fungování velice jednoduché. Sestávají ze dvou částí, ta lehčí a menší část (obvykle drobný magnet) je obvykle připevněna na pohyblivou část zařízení (dveře, okno, vrata, ...), ta větší (obvykle samotný snímač) je pak připevněna na fixní protikus, na nějž pohyblivá část doléhá (zárubně, podlaha pod vrata, rám držící dveře skříňky...). V případě, že jsou dveře zavřeny, pohyblivý magnet přitáhne jazýček na kontakt, který je ve fixním snímači a dojde tak, v závislosti na konstrukci kontaktu, k jeho sepnutí či rozepnutí. Tento stavový signál je pak po přenesení do ústředny touto vyhodnocen a předán ke zpracování podle nastavené logiky. Výhoda magnetických detektorů spočívá v jejich jednoduchosti, z ní vyplývající nízké ceně, také nejsou moc nápadné (dají se např. zabudovat přímo do rámu oken nebo zavrtat do masivu) a nejsou téměř vůbec energeticky náročné.

### **Ostatní plášťové detektory**

Do této kategorie spadají detekční zařízení pro zvláštní použití. Z běžně používaných lze uvést hlavně detektory rozbití skla, otřesové a náklonové detektory.

Detektory rozbití skla jsou zařízení pracující na principu detekce změny tlaku vzduchu ve střeženém prostoru. Pokročilejší detektory navíc disponují pokročilou digitální analýzou zvuku s nastavitelnou hranicí odolnosti, která využívá jevu, kdy tříštěné sklo vydává zvuk v charakteristických frekvenčních pásmech s charakteristickým amplitudovým vzorem, čímž dokáže spolehlivě eliminovat falešné poplachy.

Otřesové detektory snímající vibrace naleznou své uplatnění např. při hlídání předmětů v muzejních sbírkách, kde je nežádoucí manipulace s vystavenými předměty, při pokročilém hlídání prostor (např. zdivo kolem bankovních trezorů, hlídání dveří proti páčení, ad.), případně také při hlídání materiálů (hromada dřeva – hlídání dřeva proti krádežím). Použití těchto snímačů je vcelku univerzální, pro běžnou ochranu majetku se však příliš často nevyužívají. Vyjímkou je sféra hlídání vozidel (osobní automobily, motocykly, sněžné skútry, atp.), kde mají společně s náklonovými detektory nenahraditelnou roli. Rozdíl mezi detektorem otřesů a náklonu spočívá v tom, že otřesový detektor detekuje pouze zrychlení a je tak možné jej opatrností přelstít (např. opatrně motorku zvednout a odvézt ji mimo hlídání prostor a tam alarm odpojit), zatím co náklonový detektor hlídá svou absolutní polohu ve vztahu ke gravitačnímu působení, což sice

eliminuje předchozí problém, avšak nevýhoda těchto detektorů spočívá v nemožnosti detekovat vibrace způsobené poškozením bez pohybu (bouchnutí rukou, atp.). Nejlepší detektory tyto dva snímače kombinuje s logikou OR.

### **Environmentální detektory**

Pod tímto pojmem si může čtenář představit zařízení hlídající podmínky v daném prostředí. Může se tak jednat o teplotu (snímač: dioda / termistor), vlhkost (měření kapacity / odporu na zvláštním kalibrovaném členu), tlak (membrány), přítomnost hladiny vody (dva kontakty, při zatopení mezi nimi protéká proud), přítomnost specifického plynu (elektrochemické články, katalytické články, optická detekce lomu, ad.), přítomnost kouře nebo třeba hlídání spotřeby elektrického proudu. Všechny tyto detektory rozšiřují funkcionalitu klasického alarmu o nové funkce, které lze vzájemně logicky kombinovat, podmiňovat jejich detekcí spínání výstupních svorek a vytvořit tak kompletně automatizované funkční celky. Více o automatizaci pomocí EZS je uvedeno níže, v kapitole 3.1.5 .

### **3.1.2 Ovládání**

Každý EZS potřebuje pro svou funkci rozhraní, kterým se dorozumí se svou obsluhou. Základním rozhraním každého EZS bývá běžně číselná klávesnice s několika funkčními tlačítky, u starších systémů vybavená pouze kontrolkami, u novějších i grafickými displeji, popř. přímými ovládacími moduly (např. moduly nad klávesnicí systému Jablotron 100). V systému může být, v závislosti na použité ústředně, jedna nebo více klávesnic (často i různého typu). Prostřednictvím klávesnice je možné monitorovat stav systému, měnit jeho nastavení, uvádět v činnost jednotlivé funkce (zajišťování / odjišťování částí systému, zrušení poplachu, bypass detektorů, ovládání programovatelných výstupů, programování ústředny, ad.). Je zvykem, že každý moderní systém má minimálně jednu klávesnici s grafickým displejem. Pokud je v systému potřeba další klávesnice, lze se často setkat s neplnohodnotnými klávesnicemi, které jsou levnější, avšak postrádají některou nepotřebnou část. Např. pokud napojíme na jednu ústřednu všechny chodby a školní datacentrum a budeme je chtít obsluhovat nezávisle na sobě (aby bylo datacentrum zabezpečené pořád, ale při vstupu do něj se dal alarm v místnosti ovládat přímo na místě), můžeme do serverovny umístit sekundární klávesnici bez displeje a klidně i bez kláves, budeme-li vyžadovat pro zajištění a odjištění systému pouze přiložení RFID čipu nebo karty. Klávesnice se vyrábějí v klasickém drátovém, sběrníkovém i bezdrátovém provedení.



Právě RFID čipy a karty jsou oblíbeným ovládacím prvkem EZS, nejčastěji mezi laickou veřejností a to u EZS pro domácí použití. Nejčastěji se EZS ovládá pomocí uživatelsky jedinečného čtyřmístného číselného kódu (příp. s prefixem), jehož zadání autorizuje odjištění, popř. zajištění daných subsystémů (např. částí budovy – lze rozlišit přístupová práva pro jednotlivé uživatele). Zkratka RFID vznikla z anglického „radio frequency identification“, což ve volném překladu do češtiny znamená identifikace pomocí rádiových vln. RFID identifikace funguje na principu rádiové čtečky a bezbateriového elektronického identifikátoru, což je vlastně malý vysílač s číselným kódem uloženým v paměti čipu fungující díky energii, kterou vysílá do svého blízkého okolí vysílá čtečka. Tyto čipy nebo karty uživatelům mohou při výhradním použití zjednodušit práci, to však s sebou nese riziko použití (resp. zneužití) čipu bez vědomí uživatele. Přeci jen, kód, který má uživatel v hlavě, se (bez použití násilí) ukrást nedá. RFID čipy lze využít i pro zvýšení bezpečnosti a to autorizací pomocí kombinace zadání kódu a přiložení čipu. Toto řešení je však pro běžné použití zdlouhavé, proto se běžně využívá jen číselný kód.

Dalším ovládacím prvkem EZS může být dálkový ovladač komunikující s ústřednou šifrovaným protokolem prostřednictvím rádiových vln. Tyto ovladače mohou nést jedno nebo více ovládacích tlačítek, na které lze naprogramovat širokou paletu funkcí od zajišťování částí systému přes ovládání výstupů až po vyslání nouzového signálu.

Zvláštním případem ovladače EZS jsou bezdrátová tlačítka, která mohou vypadat buď jako zvonek (a tudíž je lze spárovat např. s vnitřními sirénami místo nákupu separátního elektrického zvonku) nebo jako klasický nástěnný vypínač. Ten však lze namontovat díky jeho bezdrátovému rozhraní kamkoliv a opět, lze mu přiřadit širokou paletu funkcí (ovládání garážových vrat, spínání čerpadla, sepnutí světel na určitý čas, atp.).

Lze se však setkat i s exotičtějšími ovládacími moduly. Jako velice užitečný a zajímavý se jeví např. modul sloužící pro vyslání signálu při dvojitým probliknutí dálkovými světly automobilu (motorčky, čtyřkolky...), do něž je zabudován. Lze si tak např. snadno otevřít bránu i garážová vrata přímo pomocí ovládacích prvků vozidla. Výhodou je, že tento modul není ani z pozice řidiče vidět a pokud člověk neví o jeho existenci, dále s kterým systémem je spárován, a přesnou metodu obsluhy, je jeho zabudování velmi bezpečné i do auta stojícího před domem.

Dalším, snad nejdůležitějším, komunikačním rozhraním moderního EZS je mobilní a datový komunikátor. Detailnější pozornost je tomuto zařízení věnována v kapitole 3.1.4, avšak v této sekci je důležité vědět, že přináší uživateli možnost ovládat systém prostřednictvím volání (hlasový automat) či SMS ve správném tvaru z autorizovaných telefonních čísel. Uživatel tak může prostřednictvím tohoto zařízení na dálku řídit vytápění objektu, popř. si otevřít vrata

prozvoněním. Kreativitě instalačních techniků se v oblasti dálkově spínaných relé výstupů meze nekladou. Je tak možné se v praxi setkat s velmi kreativními řešeními, jako předvedl např. pan Ladislav Folberger, který vyhrál cenu za „kompletní přístupový systém bytového domu včetně řešení pro vyúčtování za praní a sušení ve společné prádelně“.<sup>25</sup>

Skrze datový komunikátor je pak u moderních alarmů možné ovládat systém i z cloudu, a to prostřednictvím webového rozhraní či mobilní aplikace. Tyto systémy doznávají v posledních letech velmi rapidního rozvoje a v současnosti nabízí uživatelům krom ovládaní stavu zabezpečení i možnost přímo ovládat programovatelné výstupy, prohlížet historii uživatelských akcí nebo pohled do místnosti.

### 3.1.3 Analýza

Základním stavebním kamenem celého systému je pak ústředna. Základní úlohou ústředny EZS je sbírat vstupní data z detektorů a ovládacích prvků systému, částečně jim zajišťovat napájení, na základě programového nastavení provádět logické operace s těmito vstupními daty a poskytnout na základě analýzy relevantní výstup. Z pohledu oboru automatizace se jedná o řídicí člen automatizovaného systému.

Výstupem z ústředny lze rozumět logické vyhlášení poplachu, sepnutí sirén, ovládaní programovatelných výstupů nebo textový či grafický výpis informací na displej ovládací klávesnice.

Ústředna samotná se obvykle skládá z několika modulů:

- napájení
  - tuto část tvoří akumulátorem zálohovaný napájecí zdroj s řídicí elektronikou pro dobíjení, akumulátor je volen podle požadované míry zabezpečení, systém by měl fungovat bez napájení min. 12 hodin
  - může, ale nemusí napájet detektory a ovládací prvky, ty mohou mít napájení řešeno z jiného zdroje s vlastním nezávislým zálohováním pro případ výpadku sítě
- logická jednotka se svorkovnicí drátových vstupů a výstupů

---

25 Výsledky 3. ročníku soutěže Vychytávka s JABLOTRON 100. Jablotron [online]. Jablonec nad Nisou, 2016 [cit. 2017-04-06]. Dostupné z: <http://www.jablotron.com/cz/pro-montery-alarmu/sekce/aktuality/vysledky-3-rocniku-souteze-vychytavka-s-jablotron-100/>

- srdce systému, zde probíhá veškeré rozhodování a nastavování
- komunikátor (viz následující kapitola)
- volitelně: rádiový modul
  - spojuje ústřednu s bezdrátovými prvky systému

Ústřednu je nutno umístit do střezného prostoru, optimálně tam, kde nebude snadno k nalezení. Je to právě ústředna, která v případě poplachu musí informovat okolní svět o nastalé situaci. V případě vloupání do objektu je tak vhodné, aby ji lupič nenašel a nevyřadil z provozu dříve, než stihne odeslat informace na pult centrální ochrany, popř. majitelům objektu prostřednictvím SMS zpráv nebo hlasového volání. Ústředna je obvykle umístěna v ochranné krabici, která je zabezpečena proti neoprávněným zásahům tamper kontaktem, který při neoprávněném otevření ústředny vyhlásí poplach.

Pro zajištění spolehlivé funkcionality by měly být ústředny pravidelně kontrolovány servisním technikem.

Rozbor jednotlivých funkcí ústředen, které se navíc v závislosti na výrobcí a konkrétním modelu liší, by pravděpodobně zabral rozsah celé této práce (ne-li násobně více). Cílem této části práce je pouze přiblížit technické možnosti EZS a připravit tak podklad pro hlavní výzkum. Detailnímu popisu funkcí tudíž nebude věnována pozornost.

### **3.1.4 Komunikace**

Každý EZS musí disponovat komunikačním rozhraním pro přenos stavových a poplachových zpráv na příslušná místa. Tuto roli obstarává výhradně ústředna EZS skrze specializovaný **komunikátor**. V minulosti disponovaly ústředny pouze komunikátorem pro pevnou veřejnou telefonní síť, což však přinášelo poměrně vysoké náklady na provoz linky. Z tohoto důvodu se s rozvojem komunikačních sítí postupně přecházelo na modernější komunikační metody. V současnosti lze využít krom starého telefonního systému i modernější typy komunikátorů:

- mobilní hlasový + EDGE/3G/LTE data
- LAN komunikátor

Oba typy komunikátorů slouží primárně k přenosu datových zpráv na pult centrální ochrany (dále jen „PCO“). Jsou však případy, kdy se (např. z ekonomických důvodů) EZS na PCO

nepřipojuje. V tom případě nelze LAN komunikátor využít a pro přenos zpráv uživateli je možné využít pouze hlasové volání (kdy komunikátor přečte uživateli přednastavenou informaci) nebo častěji SMS zprávy obsahující stručný popis nastalé situace. K tomu potřebný mobilní komunikátor vyžaduje ke svému provozu signál mobilního operátora, SIM kartu operátora, který má v dané oblasti nejlepší signál a na SIM kartu vázaný příslušný tarif. Dnes většina operátorů nabízí zákazníkům pořízení tzv. machine2machine tarifů určených právě pro tato zařízení, kdy měsíční paušál stojí 0,- Kč a zákazník hradí pouze zvýhodněnou sazbu za využití služby (odeslané SMS, provolané minuty, data nad limit). Nejlepší podmínky pro provoz však zákazník získá nejčastěji právě připojením EZS na PCO, kdy provozovatel PCO má vyjednány s operátory výhodné podmínky a zákazník tak za službu hlídání přes PCO nezaplatí o tolik víc, než kdyby provozoval zařízení sám (ceny se pohybují řádově ve stovkách korun měsíčně podle nasmlouvané služby).

Důležitým komunikačním prvkem alarmů jsou také sirény. Ty se vyrábějí ve vnitřním a vnějším provedení a lze je využít k různým účelům. Pro vytvoření obrázku o možnostech implementace sirén následuje kazuistika: Autor v domě svých rodičů implementoval systém s dvěma vnitřními a jednou vnější sirénou. Obě vnitřní sirény jsou spárovány s bezdrátovým zvonkovým tlačítkem, na které reagují s různou hlasitostí a stejnou melodií. Siréna v domě je nastavena na nižší hlasitost, siréna v garáži (která jde slyšet z dílny) pak na vyšší. Obě mají pro toto tlačítko nastavenou stejnou melodii a reagují ve stejný okamžik. Na obou sirénách je k dispozici také kontrolka, která indikuje trvalým svitem zajištění libovolné části systému. Siréna v garáži je pak spárována s čtyřtlačítkovým dálkovým ovladačem. Dvě tlačítka slouží k zapnutí a vypnutí zahradního čerpadla, přičemž pro každé tlačítko je na siréně nastavena jiná melodie (stoupavá pro zapnutí a klesavá pro vypnutí – siréna jde ze zahrady slyšet). Zbylá dvě tlačítka slouží jako dálkové ovládání garážových vrat, které reagují také na prozvonění alarmu. Zvednutí a dosednutí vrat je indikováno pípnutím sirény v garáži iniciované koncovým magnetickým detektorem pod vraty. Obě sirény slouží dále k indikaci příchodového a odchodového zpoždění a také libovolného poplachu. Vnější siréna slouží krom poplachové indikace také k potvrzení celkového zajištění objektu krátkým pípnutím. Toto pípnutí pak mohou zaregistrovat sousedé a vědí, že je obyvatel domu na odchodu.

### 3.1.5 Řízení programovatelných výstupů

S rozvojem EZS začaly ústředny podporovat i jiné úkoly, než je hlídání majetku. Moderní ústředna tak např. dokáže krom bezpečnostních funkcí zastat i roli domovní automatizační jednotky, centrály pro cloudový monitoring environmentálních parametrů nebo ústředny pro dálkové ovládání elektrických zařízení v rámci objektu. Lze tak například docílit toho, že pohybové čidlo hlídající elektrické dveře může přes den otevírat odcházejícím lidem, zatím co v noci je hlídá proti potenciálním zlodějům. Taktéž je možné např. napojit magnetickým kontaktem hlídané okno na logiku vytápění, kdy při otevření okna bude vypnuto topení v dané místnosti za účelem úspory energií (dosažení krátkého efektivního větrání). Jen pohybové a magnetické detektory však k tvorbě pokročilých systémů nestačí. K EZS je možné připojit i již zmiňované environmentální detektory. Jejich prostřednictvím dokážeme pozvednout úroveň funkčnosti na úplně jinou úroveň. Podívejme se proto místo teoretizování na konkrétní modelové situace využití environmentálních detektorů pro alternativní funkce EZS:

- detektor teploty vzduchu
  - hlídání funkcionality vytápění / chlazení
    - při poklesu teploty pod nastavenou hranici pošli varovnou SMS
    - pokud se teplota v prostoru v zajištěném stavu zvýší, vyhleš poplach (někdo zatopil v objektu; v serverovnách pro hlídání funkce klimatizace; hlídání funkčnosti chladících zařízení (např. v obchodech hlídání chladniček s jogurty...))
  - datalogger údajů o teplotě
    - zaznamenávej do grafu průběhu teploty (dnes již možno prohlížet historická data v přehledných grafech v cloudu, přístup přes webové rozhraní či mobilní aplikaci), možno využít pro vnitřní i vnější teploty, lze tak vytvořit jednoduchou meteostanici, popř. dokumentaci
  - hlídání funkce chladících zařízení
    - při zvýšení teploty nad danou mez pošli varovnou SMS
    - zaznamenávej do grafu
- detektor vlhkosti vzduchu
  - při zvýšení vlhkosti nad limitní mez pošli varovnou SMS

- při zvýšení vlhkosti nad limitní mez v zajištěném stavu aktivuj výstupní svorku 3 (přes relé připojené topení, vhodné pro neobývané vlhké prostory)
- při poklesu vlhkosti pod nastavenou úroveň vypni výstupní svorku 3
- detektor tlaku v topném systému připojený přes analogový detektorový vstup
  - hlídání topných systémů
    - při zvýšení či poklesu tlaku mimo stanovené meze dojde k rozepnutí kontaktu  
→ vypni výstupní svorku 9 (plynový kotel)
    - je-li sepnuta výstupní svorka 6 a hodnota na čidle teploty je vyšší, než 75°C, zapni výstupní svorku 7 (pomocné čerpadlo pro krb) a pošli výstražnou SMS
  - ochrana systému čerpadla vody
    - pokud je aktivována výstupní svorka 5 a na detektoru (čerpadlo vody) a zároveň není ani po 10 sekundách sepnut tlakový spínač, vypni svorku 5
- detektor vodní hladiny
  - ochrana proti úniku vody
    - pokud je detekována vodní hladina na kterémkoliv spínači (umístěny v domě na kritických místech – koupelny, WC, u pračky, pod dřezem, pod myčkou, atp.), sepní svorku 10 (centrální blokovací solenoid přívodu vody do objektu), vyhlásí technický poplach a pošli SMS
  - napouštěcí snímač
    - pokud není v jezírku dostatek vody (snímač nedetekuje hladinu alespoň 5 minut), sepní svorku 11 (napouštěcí čerpadlo pro jezírko)
    - pokud je spínač sepnut alespoň minutu, rozepni svorku 11
- detektory plynů (CO, CNG, LPG), požární detektory (kouřové / teplotní / kombinované)
  - při detekci problému spust' technický poplach, spust' všechny interní i externí sirény, pošli výstražné SMS

Veškerá funkcionalita těchto detektorů je pouze vstupní informací pro ústřednu EZS, která řídí výstupní periferie v závislosti na přednastavené logice zpracování. Záleží tak na daném modelu

ústředny s čím vším si dokáže poradit, leckdy dokonce také na verzi firmwaru dané ústředny, jelikož výrobci své výrobky neustále zdokonalují. Je však dobré držet na paměti, že pořízení sebelepší ústředny EZS čistě pro účely automatizace se nevyplatí. Její použití však umožňuje sloučit nezávislé systémy pod jediný komplexní celek a jejich využití se jeví v rámci integrace jako žádoucí.

### **3.1.6 Shrnutí oddílu**

Je zřejmé, že správně realizovaný EZS dokáže zvýšit nejen bezpečnost budov a tím prakticky vyloučit riziko krádeží (alespoň při správném využívání), ale že dokáže v lecčem i zlepšit komfort a přehled při jejich využívání. Prvotní investice se tak může v případě jinak včas nezjistitelného problému rychle vrátit finančně (požární či tepelná čidla), v případě detekce přítomnosti oxidu uhelnatého dokonce i v životech (vlastní zkušenost autora: špatné provedení komínu karmy v kabinetu chemie vedlo k lehké otravě šesti učitelů, kteří však naštěstí příznaky na sobě včas rozpoznali – typický příklad nebezpečné situace vylučitelné adekvátním detektorem).

## **3.2 Elektronické vstupní systémy**

Elektronické vstupní systémy (EVS), nebo také lidověji přístupové systémy, jsou zařízení sloužící k zabezpečení prostor proti vstupu neoprávněných lidí, popř. k časovému omezení přístupu osob do daných prostor. Své pole působnosti naleznou v objektech, kde se pohybuje velké množství lidí, přičemž je potřeba je rozdělit na skupiny podle přístupových oprávnění, dále ve veřejně přístupných prostorech sousedícími s prostory s omezeným přístupem a v prostorech, kde je nutné monitorovat identitu a čas průchodu lidí vcházejících či vycházejících z hlídaných prostor. Kromě průchodu osob je častým jevem i kontrola průjezdu vozidel.

Přínos EVS pro školní prostředí spočívá hlavně ve zlepšení bezpečnosti skrze ztížení páchání trestné činnosti v interiérech školních budov vlivem dohledatelnosti identity vpuštěných osob. V kombinaci s opatřením stanovujícím zodpovědnost za škody způsobené umožněním vstupu neoprávněných osob tak lze efektivně vynutit kontrolu přístupu osob. Vždy však záleží na provedení, které se odvíjí od míry bezpečnostního rizika. Jako ideální a z pohledu bezpečnosti nutný prvek ochrany se jeví kombinace EVS s kamerovým systémem zlepšujícím dohledatelnost případných pachatelů.

EVS lze obecně velmi dobře přizpůsobit požadavkům každé organizace. Firem nabízejících různá řešení EVS je na trhu dostatek, konkurence v tomto odvětví vedla k diverzifikaci specifik provedení jednotlivých řešení, podle kterých se odvíjí i cena. Obecně jsou ale základní funkce EVS shodné pro všechna používaná řešení. Nejčastěji se využívají pro otevírání normálně uzavřených dveří (např. formou otevření posuvných dveří, uvolnění pohybu západky nebo spuštěním dveří otočných), uvolnění turniketu, otevření průchodové branky (např. vedle turniketu), je možné je však využít např. i pro otevření brány, zvednutí závor, atd. Součástí EVS však může být i propojení s docházkovým softwarem, resp. lze říci, že EVS je ne vždy využitým podsystémem docházkových systémů. Docházkový systém je však svým dozorovým charakterem vhodný spíše pro využití v komerčním sektoru. Přestože existují školy se zavedenou automatickou evidencí docházky, např. na odborných SŠ s více budovami v areálu, který navíc žáci v rámci výuky cíleně opouštějí, ztrácí podobný systém jak efekt, tak smysl.

Proces probíhající v EVS lze popsat blokově:

identifikace → autorizace → výstup

V prvním kroku je nutné identifikovat uživatele žádajícího o povolení ke vstupu, k čemuž slouží jedinečný identifikátor. V praxi jako identifikátor slouží např. RFID identifikátory (přívěšek na klíče, karta), otisky prstů, sken sítnice oka nebo i telefony vybavené NFC. Tento identifikátor by neměl být jednoduše duplikovatelný, měl by být levný na výrobu a práce s ním by měla být jednoduchá. Ve školství se tak využívají převážně RFID karty nebo čipy, které stačí pouze přiložit ke snímači a zbytek procesu je již v režii elektroniky.

Po přečtení identifikátoru jsou data o něm předána komunikační jednotce, která bývá obvykle umístěna poblíž kontrolního prostoru (dveře, turnikety, brána, atp.) a obvykle obsluhuje dvě čtečky, každou pro jeden směr pohybu (příchod / odchod). Komunikační jednotka předá data rozšířená o datum, čas a identifikaci snímače na ověřovací server, kde proběhne zpracování a rozhodnutí o povolení či zamítnutí vstupu. Vše je ukládáno do centrálního logu událostí. Pokud je přístup povolen, komunikační jednotka dá pokyn výstupnímu modulu (obvykle relé), který sepne či rozepne příslušné ovládací kontakty, opět v závislosti na HW konfiguraci a nastavení. Obvykle je možné nastavit i dobu sepnutí, zda se jedná o impulsní či kontinuální ovládání (impuls např. pro ŘJ ovládání brány, kontinuální je pak rozepnutí magnetu držícího dveře, atd.) a akustickou notifikaci. Komunikační jednotka obvykle disponuje i interní pamětí, do které si ukládá aktuální verzi databáze povolených čipů, kterou si stahuje ve stanovených intervalech z hlavního serveru. Tato paměť pak slouží jako záloha pro případ výpadku komunikace se serverem. Nároky na propustnost sítě jsou v případě EVS naprosto minimální.



Důležitým aspektem před realizací je důkladná rozvaha nad řešením pohybu osob autorizovaných, dále pak neautorizovaných vyjímek bez přiděleného čipu a všech osob v nouzové situaci.

V případě, že se jedná o školu mající jen jeden centrální vchod, je situace vcelku jednoduchá. Vchod může být standardně opatřen snímači, které budou otevírat dveře žákům a zaměstnancům, vedle něj lze umístit zvonek s domovním videotelefonem a elektrický zámek pak spojit nezávisle s oběma systémy (popř. skrze telefonní dveřník). Osoba na sekretariátu tak bude moci pustit do budovy návštěvy, jejichž identitu si může ověřit na obrazovce videotelefonu, autorizované osoby se do budovy dostanou i bez jejího vědomí. Problém však nastává v případě, že se do budovy bude chtít dostat neautorizovaná osoba, např. s úmyslem krást. Je zde vysoká pravděpodobnost, že v momentě, kdy tato osoba spatří, že je v budově instalován EVS, si své úmysly zkrátka rozmyslí. Pokud si je však nerozmyslí a do budovy se dostane (např. když tuto osobu vpustí žáci), bude mít problém se nepozorovaně dostat ven, jelikož je hlídán i odchod z budovy a použití nouzového tlačítka spouští poplach. Z bezpečnostního hlediska je řízení přístupu do budovy prostřednictvím blokování dveří nevyhovující, jelikož otevření dveří umožní průchod prakticky neomezenému počtu osob bez nutnosti identifikace všech kromě prvního. Člověk, který se do budovy bude chtít dostat, se tak může schovat např. mezi ostatní žáky. Tento problém se dá řešit např. identifikací pomocí turniketů, ty však zase v nouzové situaci mohou znemožnit rychlou evakuaci osob. V případě školy s více vchody pak lze operovat s omezením vstupu pro žáky skrze jediný, turniketem hlídáný vchod. Ostatní pak mohou sloužit pouze jako evakuační cesty, popř. vchody vyhrazené pro zaměstnance či návštěvy. Vždy je však potřeba vyřešit jak budou návštěvy odcházet (např. zřízení odchodových čipů se schránkou pod snímačem) a vyškolit jak žáky tak pedagogy v chování při nouzových situacích. Pro tyto se u každých blokováných odchodových dveří nebo turniketu zřizuje krabička s klíčem, popř. nouzové tlačítko pro odblokování zádržného systému. Rovněž je nutné nezapomenout na komunikaci s externími subjekty se zájmy v objektu školy, např. zásobování automatů na jídlo a pití, nájemníky tělocvičen, autoškoly, aj.

Z výše popsaných důvodů lze EVS ve školách, kde jsou systémy prakticky vždy realizovány jen pomocí blokování dveří, pokládat pouze za základní stupeň ochrany, na který nelze 100% spoléhat. Škola je ze své podstaty veřejná instituce a kdo chce, do školy si cestu najde vždy. I tak je však každá překážka bránící pachatelům trestné činnosti pro školu přínosem.

Po útoku ve škole ve Žďáru nad Sázavou v říjnu roku 2014 reagovalo na bezpečnostní situaci ve školách MŠMT vydáním dokumentu nazvaného „Metodické doporučení

k bezpečnosti dětí, žáků a studentů ve školách a školských zařízeních – Minimální standard bezpečnosti“. V tomto dokumentu (příloha č. 2) je popsána řada doporučených opatření k prevenci podobných situací. Ač lze dokument považovat za reakci vynucenou spíše než podloženými fakty tlakem veřejnosti a mediální hysterií, jež se po nepředvídatelném útoku psychicky labilní ženy rozjela na plný plyn, přináší několik velmi pozoruhodných nápadů na zlepšení bezpečnosti ve školách. Kromě upozornění technických laiků na důležitost EVS a EZS totiž navrhuje např. zvýšení noční bezpečnosti prostřednictvím pohybově spínaných reflektorů, využití bezpečnostních zámků nebo zřízení vrátnice personálně obsazené díky finančním dotacím Úřadu Práce ČR.

Ačkoliv dle vyjádření MŠMT není tento metodický materiál právně závazný a ačkoliv MŠMT již v tomto dokumentu uvádí:

*„Ministerstvo upozorňuje, že toto metodické doporučení bude aktualizováno poté, co nabude účinnosti připravovaná vyhláška o opatřeních k zajištění bezpečnosti a ochrany zdraví dětí, žáků a studentů ve školách a školských zařízeních“,*

je podstatné vědět, že k dubnu 2017 žádná podobná vyhláška neexistuje (údajně primárně kvůli několika personálním změnám na MŠMT), nicméně autor všem případným čtenářům z řad vedení škol doporučuje tento materiál důkladně prostudovat.

### **3.3 Kamerové systémy**

Ve většině budov ohledně jejich přítomnosti není zvykem ani pohnout brvou. Jsou v obchodech, bankách, na čerpacích stanicích, na náměstích. Ve školství se však okolo přínosu kamerových systémů vedou již delší čas značně kontroverzní debaty. Z pohledu autora je však přítomnost kvalitního kamerového systému ve vybraných prostorech školských zařízení nutností. Představme si tedy jak fungují.

Kamerový systém sestává z následujících částí:

- kamery
- napájení
- přenosové trasy
- analýza a záznam

- úložiště

Bezpečnostní kamery je možné rozdělit do tří v ČR běžně používaných skupin:

- analogové kamery
- HD-SDI
- IP kamery

Následující řádky shrnují stručný popis jednotlivých skupin. Vzhledem k rozdílům mezi systémy budou jednotlivé části systému vysvětleny u každé z nich.

### **Analogový systém**

Evolučně nejstarším typem kamer jsou kamery analogové. Tyto kamery využívají přenosu vysokofrekvenčního signálu skrze koaxiální kabel. Kódování obrazu probíhá podle kódovacího standardu PAL (evropská norma; rozlišení 720×576; 25 fps – fq. obrazu vychází z fq. rozvodné sítě (50 Hz) – redukuje blikání zářivek, apod.), popř. NTSC (rozlišení 720×480; americká norma, 30 fps (60Hz síť)). Obraz je snímán polovodičovým čipem (CCD/CMOS) po bodech v řádcích, systém přenosu lze přirovnat ke čtení knihy písmeno po písmenu. Signál je elektronikou převáděn na body a přenesen podle daného standardu po koaxiálním kabelu do zařízení pro zpracování obrazu.

Napájení kamer je zajištěno separátním dvoužilovým přívodem (nejčastěji 12 V), někdy si však montéři práci zjednodušovali a snižovali náklady tím, že využili stínění koaxiálního kabelu jako vedení (-) pólu zdroje a (+) pól navedli pouze jednožilovým vodičem. Jako vhodné se jeví vyvedení napájení z místa zpracování signálu.

Zpracování může probíhat různými způsoby. Každý systém (včetně níže jmenovaných) může mít tři režimy funkce:

Pokud systém slouží pouze k živému dohledu nad situací, je obraz přenášen přímo na zobrazovač (televize, monitory, projekční stěny, ...). V tomto režimu je také možné využít multiplexerů, které zkombinují obraz z více kamer na jediný zobrazovač.

Kamerový systém může fungovat i v režimu pouze pro nahrávání. K tomu slouží buď počítač s televizní kartou s více vstupy nebo specializované zařízení (nejčastěji běžící na proprietárně upravené linuxové distribuci), které zajišťuje nahrávání z více vstupů na záznamové médium. Buď se pak může jednat o záznam na videokazety (analogový záznam, nejstarší varianta), optické disky (DVD / BD) nebo již pár let nejčastěji na pevné disky či disková pole. Výjimečně se lze setkat i se záznamem na datové archivační pásky, jejichž výhoda spočívá v nízké ceně a vysoké kapacitě.

Nejčastěji se však lze setkat s řešením kombinujícím obě předchozí. Jedná se tak o systém pořizující záznam ze všech kamer za současného zobrazení snímaného obrazu v reálném čase.

Analogové kamerové systémy jsou v současnosti již zastaralým a parametricky nevyhovujícím řešením, které se buď doprodává, popř. vyrábí pouze za účelem nahrazování jinak vyhovujících starších instalací. Hlavní nevýhodou je nutnost samostatného napájení, nutnost využití drahých a na instalaci náročných koaxiálních kabelů s limitovaným poloměrem ohybu, ale hlavně nízké rozlišení a mizivá kvalita obrazu.

## **Systémy HD-SDI**

Řešení skrývající se pod zkratkou HD-SDI je systém vyvinutý za účelem modernizace dnes již zastaralých analogových systémů. Tento systém je přesně definován standardem SMPTE 292M. Systém umožňuje nasadit moderní techniku snímání, zpracování a analýzy obrazu, to vše s rozlišením Full HD (1920×1080 px).

Přenos obrazu probíhá prostřednictvím digitálního kódování: „Na přenášená data se aplikuje detekce chyb a obnova ztracených dat v podobě Hammingova kódování s paritou a paritním bitem, umožňující nejen detekci chybějících datových jednotek, ale i určení jejich pozice při přenosu.“

Rychlost přenosu je 1,485 Gbit/s a podporovány jsou snímkovací frekvence 60 Hz, 50 Hz, 30 Hz, 25 Hz a 24 Hz. Běžně se však v případě kamerových systémů lze setkat s frekvencí 25 Hz a to kvůli již popisovanému jevu reakce na blikání zářivek, apod.<sup>26</sup>

Kamery samotné tak mohou díky aplikované metodě přenosu disponovat mnohem kvalitnějšími čipy a vyšším rozlišením – a půjde to na konci poznat. Výsledný obraz je díky

---

<sup>26</sup> SDI a ti druzí, aneb na čem frčí profíci: SDI a jeho varianty. TV Freak [online]. Brno: OxyOnline, 2011 [cit. 2017-04-06]. Dostupné z: <http://www.tvfreak.cz/sdi-a-ti-druzi-aneb-na-cem-frci-profici/4521-2>

vysokorychlostnímu digitálnímu přenosu kvalitnější oproti analogovým systémům i v důsledku absence chyb způsobených elektromagnetickým rušením přenosové a trasy a vstupních obvodů zpracování.

Napájení kamer je možno provést jak samostatně, tak nově i po koaxiálním kabelu (dle modelu může být nutné využít injektoru).

Zařízení pro zpracování obrazu je z vnějšku velmi podobné analogovým systémům, uvnitř jsou však mnohem složitější. Přestože se jedná o přenos obrazových dat přes stejné médium, rekordéry musí disponovat jednak dekodérem digitálního signálu, také ale vysokým výpočetním výkonem pro zpracování několika zdrojů digitálního obrazu ve Full HD. Nároky na úložiště jsou kvůli vysokému rozlišení a tudíž i datovému toku rovněž mnohem větší. Případný recoding za účelem komprese videa do modernějších formátů, než produkují instalované kamery, pak přináší další zvýšené nároky na výpočetní výkon, což může úplně vyloučit využití některých modelů běžných rekordérů.

## **IP kamery**

Nejmodernější zařízení na trhu technologií pro obrazový záznam a dohled jsou IP systémy. Jak již zkratka IP resp., její plné znění – internet protocol – napovídají, jedná se o kamery využívající k přenosu a zpracování klasické datové sítě. Zapojením kamer do datových sítí tudíž můžeme vyřešit několik problémů současně:

Pro napájení kamer lze využít standardů definujících rozhraní Power over Ethernet, zkráceně také PoE. Jedná se o sérii postupně vyvíjených standardů pro centrální napájení aktivních prvků datových sítí, kdy data i napájení jsou přiváděny jediným kabelem. Nejstarším z této série je standard IEEE 802.3af zavedený v roce 2003, který definuje napájení pro zařízení do výkonu 15,4 W při použití stejnosměrného napětí v rozmezí 44-57 V na straně napáječe a 37-57 V na straně spotřebiče. Každý port by podle 802.3af měl být schopen dodat 350 mA a odpor kabelu by měl činit maximálně 20  $\Omega$ . Jelikož však od roku 2003 zaznamenala síťová zařízení prudký rozvoj, někdy už toto napájení přestávalo stačit. Organizace IEEE tak začala připravovat nové řešení. Nástupníkem se staly napřed v roce 2009 standard 802.3at, označovaný také jako PoE+, kde jsou definovány hodnoty napětí 50-57 V na straně napáječe (tj. nárůst minimální hodnoty o 6 V) a 42,5-57 V na straně spotřebiče (nárůst minimální hodnoty o 5,5 V). Každý port by měl zvládnout dodat minimálně 600 mA, přičemž celkový výkon zdroje by neměl per port překročit 30 W. V současnosti výrobci experimentují s novým standardem 802.3bt, který

by měl zařízením umožnit čerpat výkon až na hranici 100 W. Standardně podporované rychlosti jsou do 1 Gbit, což však neznamená, že není možné najít proprietární zařízení schopné napájet i rychlejší datové linky. PoE zařízení se dělí na aktivní a pasivní, kdy aktivní zařízení jsou schopna vzájemné komunikace za účelem vyjednání adekvátního napájení (zařízení si požádá o předdefinovanou mez výkonu, případně v portu switche může fungovat i zařízení bez PoE), zatímco pasivní injektory dodávají napětí konstantně a pokud do něj připojíme zařízení bez PoE, můžeme jej zničit. Taktéž je vhodné nést v paměti fakt, že zařízení různých výrobců, za vše např. Mikrotik a Ubiquiti Networks, využívají proprietární implementaci PoE s napětíovou hladinou pouze 24 V. Připojení takto napájených zařízení na standardní 48V PoE by tak znamenalo s největší pravděpodobností jejich destrukci (Mikrotik mívá rating pouze do 28 V).

Dalším z problémů, které můžeme vyřešit využitím IP technologie, je eliminace potřeby natažení zvláštních rozvodů pro kamery koaxiálními kabely. Existuje-li v daném místě rozvod strukturované kabeláže, můžeme veškerá data přenášet prostřednictvím ní. Do budoucna plánovaný kamerový systém je tak možné přichystat předem jako součást větší rekonstrukce. Pár set metrů kabeláže navíc pro kamery je v rozpočtu na rekonstrukci elektroinstalace minoritní položka.

Markantní výhodou je i eliminace potřeby zvláštních páteřních vedení, takže kamery je možné jednoduše nainstalovat i na sousedních budovách spojených s hlavní budovou páteřní datovou trasou. Veškerá komunikace IP kamer totiž probíhá standardní datovou komunikací přes standardní switche. Je však nutné dát si pozor na zvýšené nároky na odezvu a propustnost datových kanálů pro tyto kamery. Rovněž se z bezpečnostních důvodů jeví jako velmi vhodné využít pro přenos jejich komunikace separátní virtuální síť (VLAN).

Velkým rozdílem mezi IP a analogovými systémy je elektronika uvnitř kamer samotných. Zatím co u analogových kamer se zpracování nejčastěji provádí až na záznamovém zařízení, pokud vůbec, u každé IP kamery probíhá určitá míra zpracování obrazu již v kameře samotné. Data ze snímače se převádějí na obraz, který je následně kódován integrovanou výpočetní jednotkou do digitálního streamu odesílaného prostřednictvím síťového rozhraní. Formát streamu je vlastností kamery, starší IP kamery využívaly kodeku MJPEG, později bylo možné se setkat s MPEG-4, v současnosti je běžným standardem kodek H.264, pomalu se však přechází na H.265. Rozdíl mezi těmito kodeky pozná koncový uživatel hlavně na kvalitě záznamu při zachování rychlosti datového toku (konst. bitrate), zatížení sítě a velikosti souborů se záznamem, což se projeví ve snížených nárocích na úložiště záznamu. Srovnáme-li nároky na úložný prostor

pro jednu hodinu záznamu z jediné kamery, dojdeme k následujícím hodnotám (pouze orientační, liší se vždy dle použitého algoritmu):

2048×1536 px (3 MPx) @ 25 fps

- MJPEG: ~ 125 GB
- MPEG-2: ~ 25 GB
- MPEG-4: ~ 14 GB
- H.264 (AVC): ~ 9 GB
- H.265 (HEVC): ~ 4 GB
  - vychází z tvrzení: „*The overall average bit rate saving achieved by HEVC compared to AVC for the same subjective quality was found to be 59% as supposed to the 44% gain shown with objective quality metrics.*“<sup>27</sup>

Všechny kamery nezávisle na výše uvedených skupinách se kromě rozlišení (a výstupního formátu v případě IP) liší také v dalších parametrech. Mezi hlavní patří velikost snímače, kvalita a světelnost optické soustavy a přítomnost WDR. Větší snímač se světelnější optickou soustavou zajistí více fotonů dopadajících na polovodič s plochou jednoho pixelu, což umožní získat kvalitnější obraz v horších světelných podmínkách díky menšímu výstupnímu šumu (není nutno tolik předzesilovat získaný signál rušený poruchovými vlivy – vlastní vodivost, různé druhy emg rušení, kosmické záření, přirozená radioaktivita, volné radikály, etc.). Ve spojení s WDR (wide dynamic range), což je funkce zvětšující dynamický rozsah obrazu a automatickými odklopnými IR filtry tak lze dosáhnout vysoce kvalitních záběrů i za špatných podmínek pro snímání (přesvětlení, slunce v záběru (zdroj silného IR záření), nedostatek světla, protisvětlo). Každý výrobce přidává do svých výrobků různou proprietární funkcionalitu, na trhu je tak možné nalézt řešení prakticky jakéhokoliv problému, ta pokročilá si však výrobci nechají rádi zaplatit.

## Umístění kamer

Autor zastává názor, že z důvodu efektivní ochrany majetku by neměly kamery chybět u žádného vchodu do školní budovy (včetně běžně uzamčených, avšak sloužících např. jako únikové cesty),

---

<sup>27</sup> H.265/HEVC vs H.264/AVC: 50% bit rate savings verified. BBC - Research and Development [online]. London: BBC, 2017 [cit. 2017-04-06]. Dostupné z: <http://www.bbc.co.uk/rd/blog/2016-01-h-dot-265-slash-hevc-vs-h-dot-264-slash-avc-50-percent-bit-rate-savings-verified>

dále na příjezdových cestách na pozemky školy a v případě větších chodeb i zde. Tímto lze efektivně pokrýt veškeré prostory školy i bez zasahování do soukromí osob, na což je nutné brát zvláštní zřetel. Demonstrujme to na kazuistice: Častým problémem ve školách bez přístupových systémů jsou krádeže ze šaten tělocvičen v odpoledních hodinách, kdy je škola již prázdná a tělocvična se pronajímá externím zájemcům, škola tou dobou bývá leckdy otevřená. Krádeže ze šaten lze eliminovat kombinací přístupového a kamerového systému, je však nežádoucí a nezákonné umisťovat kamery tak, aby zabíraly prostory šaten samotných. Jako vhodné se jeví jejich umístění na příchodové cesty k šatnám včetně bočního záběru na vchodové dveře do této místnosti. Z těchto záběrů je ve většině případů zřetelně vidět kdo do prostor vstoupil, jak (zda např. nevyužil páčidla...) a co si nese s sebou. Jako nevhodné je ve školách považováno také umístění kamer přímo ve třídách a to vzhledem k faktu, že kamery nesmí sloužit ke sledování konkrétních osob, ať už zaměstnanců školy, pedagogů nebo žáků – všem musí být zaručeno právo na adekvátní soukromí. Detailní informace týkající se této problematiky lze nalézt ve „Vyjádření a doporučení Úřadu pro ochranu osobních údajů k možnosti instalovat kamerové systémy v prostorách školy“ ze dne 12. 3. 2007, na které se MŠMT při komunikaci se školami odkazovalo i v době psaní této práce. Tento dokument je přílohou č. 3 této práce.

### **Záznamová zařízení**

Na trhu existuje široké spektrum produktů sloužících k záznamu obrazu z kamer. V roce 2017 lze záznamové systémy rozdělit na dva základní typy: dedikovaná zařízení a počítače s přídatnými kartami.

Ať už jde v době psaní této práce o záznamové zařízení pro analogové systémy, HD-SDI, méně běžné AHD nebo IP systémy, prakticky vždy jde v případě dedikovaných zařízení o miniaturizované počítače na úsporných platformách, na kterých běží výrobcem upravená proprietární distribuce Linuxu ořezaná o nepotřebné funkce. Zásadními výhodami těchto dedikovaných rekordérů jsou hlavně nízká spotřeba, malá velikost a nízká cena za nový výrobek. Rekordéry umožňují dle modelu a ceny ukládání záznamu z kamer v různých formátech (ty levnější nabízejí ukládání buď v plné nebo ve snížené kvalitě; pokročilejší umožňují i detailnější nastavení včetně počtu snímků za sekundu) a to buď na jeden nebo na více disků, popř. do síťového úložiště (SMB, FTP, SAN). V případě využití více disků, popř. v případě zařízení určených pro více kamer (12 a více) se však výhody dedikovaných rekordérů začínají vytrácet a začínají se výrazně projevovat počítačem řízených nahrávacích systémů.



V případě PC systémů je nutné pro všechny typy kamer kromě IP pořídit buď specializované rozšiřující karty, které počítači umožní využít exotických rozhraní (jako je právě analog, HD-SDI nebo AHD – tyto dekodéry v novém počítači nepotřebuje ani celé procento uživatelů), nebo lze pořídit technicky vhodnější enkodéry, které unifikují signál z nesítových kamer a převedou je na IP stream (a umožní tak lepší škálovatelnost). Výše uvedený postup je nutný proto, že v roce 2017 je běžné, že počítač disponuje 1Gbps síťovým rozhraním, rovněž se na trhu objevují první vlašťovky s 5Gbps sítí (v době psaní práce naprosto nový standard IEEE 802.3bz).<sup>28</sup>

Počítačové systémy mají oproti dedikovaným rekordérům několik markantních výhod. Jednak lze tyto systémy prakticky neomezeně rozšiřovat (když nestačí výkon 1 PC, můžeme virtualizovat cluster), zatímco u dedikovaných boxů jsme limitováni počtem kamer, který nám výrobce u daného modelu povolí. V případě modernizace kamerové technologie stačí v počítači pouze vyměnit kartu s příslušnými rozhraními (resp. ji odstranit úplně). Také můžeme pro zpracování získaného signálu využít libovolný software, který je často na rozdíl od softwaru v rekordérech aktualizován a leckdy přináší uživateli i novou funkcionalitu, výkonové a bezpečnostní optimalizace. Klasické počítače založené na architektuře x64 jsou v roce 2017 běžně dostupným obchodním artiklem a to jak nové, tak i repasované. Je tak např. možné zakoupit dva starší servery po cca. 10 tis. korun, doplnit je o síťové karty, plně virtualizovat operační systém na něm běžící (např. přes VMware ESXi), propojit je s diskovým polem a výpočty obrazových dat ponechat výkonnému virtuálnímu počítači s vědomím, že pokud budeme potřebovat přidat do systému další kamery, rozšířit cluster o další jednotku není problém. Software využívaný pro kamerové systémy může pocházet buď od komerční firmy (placené profesionální řešení s pokročilými funkcemi), od výrobce kamer (často zdarma), popř. může jít i o řešení vytvořené open source komunitou s možností dokoupit profesionální moduly. Autor preferuje využití posledně uvedeného řešení z důvodu decentralizace vývoje, dozoru bezpečnosti jeho vývoje (žádný backdoor – open-source komunity nespolupracují s tajnými službami, protože jsou založeny na veřejném přístupu k informacím – nic nelze dokonale utajit) a dobré dostupnosti specializovaných zásuvných modulů.

---

28 ASRock Debuts AM4 Motherboards With 5 Gigabit LAN. Tom's Hardware [online]. 2017 [cit. 2017-04-06]. Dostupné z: <http://www.tomshardware.com/news/asrock-amd-am4-10g-ryzen,33366.html>

## Nákup kamerového systému

V předchozích odstavcích byla řeč o spoustě parametrů kamer, záznamových zařízení, podle čeho však vybrat? Primárně podle rozpočtu, který máme k dispozici, autor doporučuje využít zásadně IP kamer. Ceny nejlevnějších a reálně použitelných kompletně statických kamer pro venkovní použití se na trhu pohybují orientačně okolo 6000,- Kč s DPH.<sup>29</sup>

Sehnat se však dají i kousky za 2000,- Kč, ty však budou mít pravděpodobně výrazné problémy s kvalitou obrazu a to jak ve dne, tak i v noci. Kamery kolem 6000,- Kč jsou částečně použitelné i v noci, nelze však od nich čekat závratnou kvalitu obrazu. Při průzkumu trhu prováděném na portálu firmy Viacom byla výše ozdrojovaná kamera v parametricky nejlepší na trhu, navíc je hojně využívána při instalacích v SOHO sektoru.

V případě požadavku na kvalitní obraz kamery i v nočních hodinách je nutno se poohlížet primárně po kamerách, které disponují většími a dražšími snímači, propracovanější elektronikou a kvalitnější optikou. Cenově tyto kamery začínají na hladině 20.000,- Kč. **(zdroj)**<sup>30</sup>

Pro zpracování autor doporučuje volit již popsané řešení založené na softwarových produktech pro PC a preferuje řešení na bázi open-source. Pro složitější instalace je samozřejmě možné využít i komerčních produktů, potřeby škol však open-sourcová řešení z naprosté většiny plně uspokojí i zcela zdarma (resp. za cenu hardware).

## 3.4 Elektronické požární systémy

Elektronické požární systémy, zkráceně také EPS, slouží pro včasnou detekci nebo hlášení vzniklého, vznikajícího nebo potenciálně možného požáru.

Každý EPS se skládá z několika základních částí:

- detekční část
- přenosové trasy
- vyhodnocovací jednotka
- komunikační systém

---

29 HIKVISION DS-2CD2342WD-I (2.8mm). Viacom [online]. 2017 [cit. 2017-04-06]. Dostupné z: <https://www.viacom.cz/hikvision-ds-2cd2342wd-i-2-8mm/product-970>

30 HIKVISION DS-2CD4125FWD-IZ (2.8-12mm). Viacom [online]. 2017 [cit. 2017-04-06]. Dostupné z: <https://www.viacom.cz/hikvision-ds-2cd4125fwd-iz-2-8-12mm/product-1087>

Jak můžeme vidět, EPS jsou základní strukturou velice podobné EZS, mají však svá specifika, která EZS nemusejí řešit.

## Detektory

Základem EPS jsou požární detektory. Ty mohou pracovat na několika základních principech.<sup>31</sup>

- kouřové optické
  - slouží k detekci kouře – snímají odraz světla od kouřových částic
- kouřové ionizační
  - snímají míru vodivosti přítomného plynu – kouřové částice kumulují náboj, změny elektrostatického pole jsou pak vyhodnocovány elektronikou
- termomaximální
  - vyhláší poplach po překročení předdefinované teploty (většinou okolo 60°C)
- termodiferenciální
  - vyhláší poplach po překročení míry oteplení (cca 8°C / min)
- plamenné (IR/UV)
  - snímají spektrum vyzařované daným plamenem, dle typu hořících látek se volí snímače pro specifická spektra
- kombinované
  - kombinují výše uvedené principy, metodika AND/OR

Životnost kouřových detektorů je uváděna mezi osmi a deseti lety.

Zvláštním případem jsou rovněž obecně známé tlačítkové hlásiče, což je principiálně pouze obyčejné sklíčkem zakryté tlačítko s případným adresním modulem sloužící k ručnímu nahlášení požáru.

Ze speciálních zařízení můžeme dále uvést systém nasávacích trubiček určených k přivedení vzduchu z analyzovaného prostoru k příslušnému detektoru. Toto řešení je vysoce

---

31 Bezpečnostní inženýrství - Detektory požárů a senzory plynů. Vysoká škola chemicko-technologická v Praze [online]. Praha, 2017 [cit. 2017-04-06]. Dostupné z: [http://uchi.vscht.cz/uploads/pedagogika/bezpecnostni\\_inzenyrstvi/09.BI.Senzory.pdf](http://uchi.vscht.cz/uploads/pedagogika/bezpecnostni_inzenyrstvi/09.BI.Senzory.pdf)

cenově efektivní, jelikož umožňuje jediným čidlem zpracovat více místností, popř. velkou plochu. Jeho nevýhoda je nepřesná lokalizace místa požáru v případě pozitivní detekce.

Další specialitou mohou být i lineární požární systémy a to např. tlakové (uzavřená měděná trubka s tlakovým čidlem) nebo optické (infrabariéra měřící malé změny v odrazivosti paprsku vysílaného proti odrazné ploše). Za zmínku stojí i možnost využití detekčních požárních kabelů (změna parametrů popř. zkrat při překročení kalibrované teploty). Výše uvedené systémy naleznou využití např. v eskalátorech, mechanických strojích nebo kabely např. pod izolací, kde je riziko skrytého požáru např. od komína.

Kromě požárních detektorů umožňují EPS, podobně jako EZS, využít pro vyvolání poplachu i již popsané environmentální detektory.

Na požár v objektu hlídaném aktivovaným EZS může, vzhledem ke svému principu, zareagovat i klasické PIR čidlo, tato čidla však nelze použít pro tyto účely cíleně.

### **Přenosové trasy**

Kabelové vedení EPS musí být dle normy ČSN EN 54-1 (342710) provedeno nehořlavými kabely, které odolávají požáru po dobu 30 minut, po které musí systém zůstat plně funkční. Zároveň si tato izolace musí i při vystavení ohni uchovat své mechanické vlastnosti a udržet vodiče separované. Stejně jako kabely musí být označeny i nehořlavé povrchové instalační krabice. Jeví se jako vysoce žádoucí, aby kabely nebyly při provozu rušeny vlivy jiných systémů, tudíž aby byly využity kabely stíněné. Za účelem eliminace nechtěných zásahů je rovněž vhodné vést kabely jinou trasou, než všechny ostatní. I proto mají tyto kabely červenou barvu a jejich izolace je vyrobena z bezhalogenových materiálů (viz popis LSZH v kapitole 3.1.1).

Vyhodnocovací jednotky jsou funkčně srovnatelné s jednotkami EZS, jediným praktickým rozdílem je jejich kompaktnost, tzn. že není využita externí klávesnice a že detektory jsou jinak adresovatelné. Vzhledem k faktu, že se většinou jedná o proprietární systémy jim zde nebude věnováno místo, stejně tak jako sirénám EZS, které jsou však umísťovány primárně do hlídaných prostor s cílem vzbudit a efektivně upozornit obyvatele na případný požár. Komunikační cesty jsou rovněž srovnatelné s EZS.

Moderním způsobem detekce požárů a dokonce i jejich předcházení je obrazová analýza prováděná kamerovými systémy, případně pouze jejich softwarovými nastavbami. V případě požáru je na obrazu možno pozorovat typický kouř (detekovatelný algoritmičticky), rovněž je

možno využít i analýzy obrazu z termokamer, které jsou schopny detekovat požár dříve, než vypukne (např. zaznamenají přehřívající se pouzdra přidírajících se ložisek v olejové lázni nebo lokálně se přehřívající části výkonných transformátorů (z čehož lze závadu přímo přisoudit konkrétní části daného vinutí)). Tento způsob je však drahý a nalézá uplatnění jen v ekonomicky oddůvodnitelných scénářích, např. v generátorových halách jaderných bloků, apod. Aplikace v sektoru školství není pravděpodobná.

### 3.5 Monitoring technologických celků

Technologické celky je vhodné zaštitit centrálním monitorovacím systémem. Tyto systémy mají za cíl včasné detekovat, popř. autonomně řešit technologické problémy v jednotlivých systémech, které nemusejí být pod neustálým dozorem.

Autor práce má několikaleté praktické zkušenosti s monitoringem systémových celků pomocí řešení pod názvem Zabbix. Jedná se opět o open-source systém založený na Linuxu (autor využívá stabilní Debian), který lze nasadit pro velmi variabilní zadání, je intuitivně spravovatelný přes moderní dynamické webové rozhraní a dokáže hlídat prakticky cokoliv, co nějakým způsobem komunikuje přes TCP/IP. Nejčastěji je systémovými administrátory využíván k dohledu nad datovými toky v síti, dostupnosti jednotlivých síťových segmentů, k dohledu nad stavem, zatížením a včasné analýze problémů serverů (automaticky provedený restart, málo místa na úložištích, nadměrné zatížení, atp.), na nich běžících aplikacích (weby, databáze, síťové služby, ...), atd. Vzhledem k častému umístění školních WiFi AP na veřejně přístupných chodbách je pro tyto účely rovněž vhodné zřídit hlídání dostupnosti s automatickými notifikacemi v případě výpadku. Tyto výpadky mohou být zapříčiněny nejen výpadkem napájení či selháním AP, ale také např. krádeží nebo sabotáží přívodní linky. Včasné řešení situace, např. prostřednictvím kamerového dohledu, je tak velmi žádoucí.

Zabbix nabízí širokou paletu předprogramovaných agentů (programů pro hlídání počítačů) a s nimi svázaných šablon pro monitorování (ping, SNMP, Windows server, Windows klient, Linux server, atp.), pomocí nichž lze monitorování daného zařízení nakonfigurovat velice rychle a efektivně. Není nutné nic složitě programovat, pro hromadné nasazení lze tyto agenty dokonce přímo implementovat do předkonfigurovaného jednotného instalačního image. Agent se následně po instalaci dokáže sám spojit se serverem Zabbixu, proskenovat konfiguraci počítače a vytvořit potřebné záznamy o existenci počítače v systému.

Za účelem zrychlení reakční doby administrátora se jako velice vhodné jeví využití SMS brány (např. Jablotron David), která v případě problému odešle přes síť veřejného telefonního operátora SMS na předdefinovaná telefonní čísla. Případné krádeže drahého telekomunikačního vybavení tak lze eliminovat již v zárodku.

Mezi další nekomerční běžně používané systémy se řadí např. Nagios (opensource nebo komerční verze), Cacti, OpenNMS a další. Autor však, vzhledem k intuitivnosti a modernosti systému (což není standardem) doporučuje využívat právě Zabbix.

## **4 Doplnkové a komfortní systémy**

### **4.1 Místní rozhlas**

Dalším technologickým celkem běžně využívaným obzvláště na školách ale třeba i v obchodních centrech je obligátně známý místní rozhlas. Vzhledem k faktu, že princip fungování místního rozhlasu je obecně známý (nejčastěji 100V sběrnice, ze které jsou napájeny paralelně připojené reproduktory), považuje autor za podstatné popsat pouze výhody, které systém škole svou přítomností přináší.

Asi nejdůležitější rolí místního (nebo lidověji také školního) rozhlasu je jeho využití jakožto hromadného sdělovacího prostředku. Z jednoho místa lze dostat s patřičnou pozorností mluvené slovo do všech zákoutí školy, což je využitelné nejen pro informativní sdělení žákům, ale např. i při hledání lidí v areálu.

Velmi důležitým a efektivním pomocníkem je rozhlas v nouzových situacích – velmi efektivně dokáže např. zabránit panice, umožnit koordinovanou evakuaci školy či informovat o nastalé nebezpečné situaci (únik plynu, aktivní střelec v budově, atd.).

V některých školách je také rozhlas využit místo klasických zvonků jako přenosové médium pro elektronické zvonění. Tento systém je vlastně pouze načasovaný přehrávač nahrávek, které jsou do zesilovače puštěny v nastavených časech. Variabilita takového systému je v době levných mikroprocesorů značná, lze tak např. jako zvonění nastavit nejrůznější melodie či zvuky nebo upozornit s předstihem krátkým tónem na blížící se konec hodiny.

Rozhlas je také v některých případech možno využít jako volitelného zdroje hudby. Lze totiž postavit rozhlasové systémy s více zvukovými okruhy (většinou 2, technické limity v tomto

případě kreativitě moc mezí nekladou). První okruh je nucený a odpovídá klasické podobě rozhlasu, tzn. když někdo mluví, mluví do všech přijmačů. Kromě toho je možné na voliči hlasitosti pro daný reproduktor možné zapnout i volitelný okruh, na kterém může být např. non-stop puštěné rádio. Tento systém jednak značně zlepší školní klima a zároveň sníží motivaci žáků o zasahování do počítačů ve třídách za účelem pouštění hudby z youtube v době přestávek.

## 4.2 Osvětlení

Velice důležitým faktorem pro výuku je nejen z hygienického hlediska kvalitní osvětlení prostor určených pro výuku. Existuje řada norem, ať už elektrikářských či hygienických, které předepisují požadavky na světelné podmínky ve třídách a v tělocvičnách.

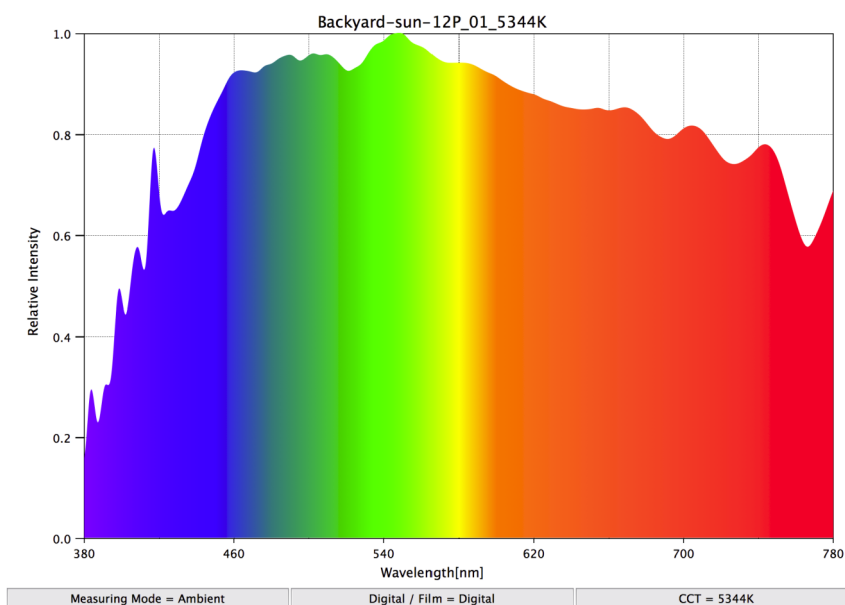
Podívejme se nyní do technické praxe. Na následujících řádcích bude pozornost věnována primárně těm školám, kde dosud plošná rekonstrukce elektroinstalace (nezřídka staré desítky let a opravované jen lokálně při výskytu problému) neproběhla a to za účelem shrnutí „dobrých mravů“ při plánování rekonstrukce osvětlení ve školách.

Lze vycházet z bodu, že vzhledem k finančním podmínkách českého školství není výjimečný stav, kdy poslední plošná rekonstrukce elektroinstalace ve spojení s plošnou výměnou svítidel proběhla ještě za éry komunismu. Z této doby se tak ve školách často dochovala ještě původní zářivková svítidla bez elektronických startérů a leckdy také ještě obyčejná svítidla žárovková.

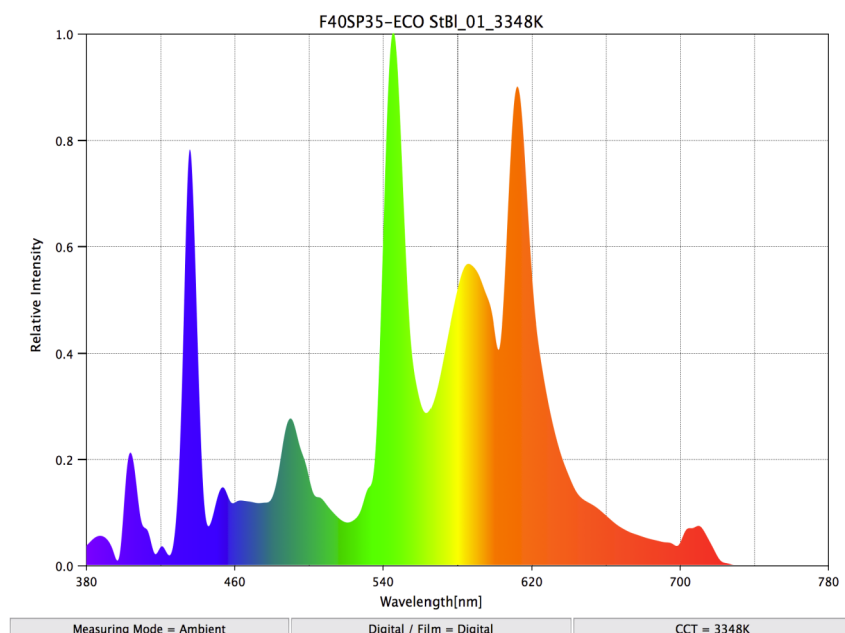
Je obecně známým faktem, že žárovková a starší zářivková svítidla mají, ve srovnání s moderními zdroji vysoké nároky na příkon. Z tohoto důvodu se, s výjimkou zvláštních případů zmíněných později, přechází na jiné světelné zdroje, nejčastěji na bázi LED diod a modernizovaných zářivek s elektronickými předřadníky.

Existuje několik zásadních rozdílů mezi starými a novými modely zářivkových trubcových svítidel. Tím hlavním je barva světla – moderní zářivkové trubice s dokáží dosáhnout běžně vyzářit světlo až v 90-98 % viditelného spektra s výraznějšími maximy v určitých jeho částech. Setkat se lze ale i s trubicemi, které jsou rády, že vůbec dosáhnou hodnot CRI okolo 50 %. Z níže uvedených grafů je patrné, že typická zářivka vyzařuje hlavní část světelného toku v zelené a modré části spektra, kterou výrazněji doplňuje pouze oranžová barva. Při porovnání se spektrem denního světla je možno spatřit evidentní rozdíl, a to, že v denním

světla velice hojně zastoupená červená barva v zářivkovém světle prakticky chybí, jak je krásně demonstrováno ve zdrojovém článku týkajícím se volby vhodného osvětlení pro účely studiové fotografie.<sup>32</sup> Autor zde uvádí několik perfektně zpracovaných spektrálních analýz.



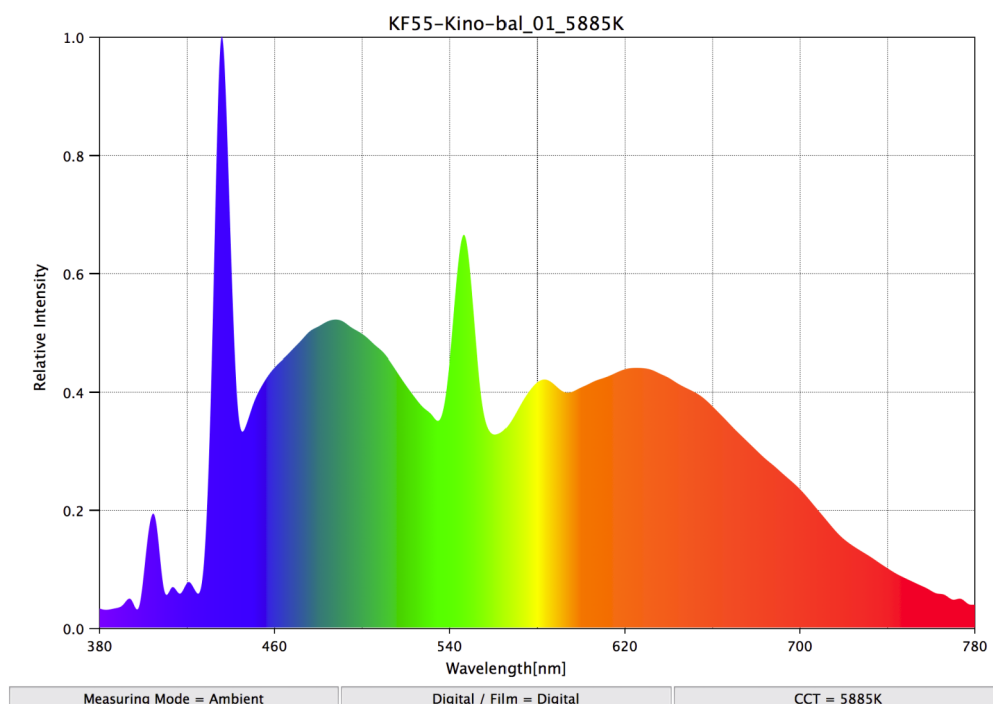
*Ilustrace 2: Spektrum denního světla (přímé slunce)*



*Ilustrace 3: Spektrum levnější zářivky*

32 Is it a good idea to build your own fluorescent video lights? Fixing a video [online]. 2015 [cit. 2017-04-09]. Dostupné z: <http://fixingyourvideo.com/wf-kino>





*Ilustrace 4: Spektrum fotografické zářivky*

Jelikož se běžně setkáme pouze se zářivkami s omezeným vyzařovaným barevným spektrem, je zářivkové světlo obecně vnímáno obecně jako velice chladné, což výrazně mění jeho výslednou percepci. Jak uvádí autor uvedeného článku u následující fotografie, obě fotografie byly barevně upraveny pro dosažení nejlepšího možného výsledku, avšak na pravé fotografii zcela chybí červené světlo, které by se mohlo odrazit od červených částí autorovy tváře.



*Ilustrace 5: Srovnání vjemu se speciální zářivkou (vlevo) a standardní levnou zářivkou (vpravo)*

Druhý důležitý rozdíl je možné spatřit ve startovacím mechanismu, kde se přechází od analogových startérů, které často rády hučely (vyhřáté tlumivky) a způsobovaly elektromagnetické rušení (jazýčkové startéry) na spínané elektronické předřadníky (dále jen „EP“) s teplým startem, které jednak zářivku rozsvítí prakticky ihned a bez blikání, jednak u toho nejdou slyšet, krom toho však také nejčastěji využívají tzv. teplý start, tj. že napřed předejde žhavené části trubice a proud do ní pustí až po nažhavení, čímž výrazně zlepšují její životnost. Moderní EP také zvládají napájet i více trubic najednou a eliminují stroboskopický efekt známý ze starších instalací, kde byly trubice přímo napájeny střídavým proudem o frekvenci 50 Hz. EP využívají principu spínaných zdrojů, kdy napřed síťový proud usměrní a vyhladí a až následně jej rozkmitají na frekvence v řádech desítek až stovek kHz. Využití EP tak oproti starým typům značně snižuje energetické ztráty.

Třetím významným rozdílem je možnost využití regulačních předřadníků, které umí zářivku stmívat, navíc je možné tyto předřadníky i programovat pro různé účely (tlačítkové spínání se stmívačem, dálkové ovládání z centrálního pultu, atp.). Toto řešení je však zbytečně komplikované a drahé a autor doporučuje pro tyto účely využít spíše jednoduše stmívatelných LED světel.

Čtvrtý rozdíl spočívá v efektivnější konstrukci svítidel. Moderní zářivková tělesa mají z většiny půl-kulově tvarované odrazné plochy z horní strany a reflexní stínící mřížky, které dokonale propouštějí vyzářované světlo pod sebe (nejčastěji v úhlu 120°), ne však plně do stran. Při pohledu nad sebe tedy člověk není oslněn, zároveň je tak světlo efektivně distribuováno tam, kde je reálně potřeba a nedochází k jeho předčasnému odrazu a pohlcení. Zářivková tělesa mají také často možnost variabilního nastavení výšky, jelikož bývají, oproti dřívější častější povrchové montáži, spouštěny na lankách ze stropních kotev.

A na závěr – žádná moderní zářivka by neměla obsahovat nebezpečné těžké kovy.

## **LED čipy**

V době psaní této práce převládal ve světě trend, kdy se svět elektrotechniky začal prudce přeorientovávat směrem od využívání klasických světelných zdrojů k plošnému zavádění světel na bázi LED čipů. Tato polovodičová technika má několik zásadních a často komerčně zdůrazňovaných výhod, také má však několik nevýhod, o kterých se již tak často nehovoří.

Jednoznačnou výhodou LED světel je jejich vysoká efektivita a energetická nenáročnost. Jak je patrné z následující tabulky <sup>33</sup>, při stejném příkonu dokáží vyprodukovat mnohem větší světelný tok (tzn. mají mnohem větší měrný světelný výkon P), než všechny běžně používané světelné zdroje. V kombinaci s nízkou hmotností, malými rozměry a nenáročností na chlazení běžně využívaných modulů je toto řešení zdánlivě svatý grál osvětlovací techniky.

<i>Měrný světelný výkon a Světelná účinnost</i>	<i>P (lm/W)</i>	<i>K (%)</i>
<i>Svíčka</i>	<i>0,3</i>	<i>0,04</i>
<i>Žárovka wolframová, 5 W</i>	<i>5</i>	<i>0,7</i>
<i>Žárovka wolframová, 40 W</i>	<i>10,5</i>	<i>1,5</i>
<i>Žárovka wolframová, 60 W</i>	<i>11,7</i>	<i>1,7</i>
<i>Žárovka wolframová, 100 W</i>	<i>13,4</i>	<i>2,0</i>
<i>Halogenová žárovka křemenná</i>	<i>24</i>	<i>3,5</i>
<i>Vysokoteplotní žárovka</i>	<i>35</i>	<i>5,1</i>
<i>Kompaktní zářivka (úsporná žárovka) 5 - 24 W</i>	<i>45 - 60</i>	<i>6,6 - 8,8</i>
<i>Zářivka trubicová</i>	<i>50 - 104</i>	<i>7 - 15,2</i>
<i>Výbojka metalhalogenidová</i>	<i>100</i>	<i>15</i>
<i>Výbojka vysokotlaká, sodíková</i>	<i>150</i>	<i>22</i>
<i>Výbojka nízkotlaká, sodíková</i>	<i>183</i>	<i>27</i>
<i>Svítilno LED20</i>	<i>do 140</i>	<i>do 20,5</i>
<i>denní světlo</i>	<i>41</i>	<i>6,0</i>

*Tab. 1: Měrný světelný výkon P v lm/W a světelná účinnost K v % pro různé zdroje světla. Údaje pro wolframové žárovky 60 W a 100 W odpovídají produkci značky PHILIPS (Polsko), která je běžně v našich obchodech. Známe-li energetický příkon zdroje ve W a vynásobíme jím měrný světelný výkon P v 2. sloupci, dostaneme celkový světelný tok zdroje v lm.*

Existuje však řada problémů, které je třeba důkladně zvážit, o kterých se mluví pouze v nejobornějších kruzích a které se ke koncovému zákazníkovi dostanou jen málokdy. Prvním problémem je opět chromatičnost světla, druhým je pokles jasu v průběhu životnosti čipu (svítidlo = 1 velký nebo více malých LED čipů), třetím problémem je životnost čipů samotných, a posledním je životnost svítidel.

V případě prvních tří uvedených problémů je rozhodujícím faktorem kvalita využití výrobní technologie, která závisí prakticky výhradně na výrobci a jeho produktové řadě. Na trhu LED čipů se vyskytuje pouze několik málo výrobců generických LED čipů, jelikož výroba

33 Světelná účinnost zdrojů světla (žárovky, kompaktní zářivky, výbojky a dalších). Stavebnictvi3000.cz: nejvíce informací o stavebnictví v ČR [online]. 2008 [cit. 2017-04-09]. Dostupné z: <http://www.stavebnictvi3000.cz/clanky/zarovka-usporna-zarovka-mnozstvi-svetla/>

polovodičové techniky není levná záležitost a koncentruje se tak výhradně do světových technologických center jako jsou Japonsko, Tchaj-wan, USA nebo Čína. Kvalitní LED čip by měl v průběhu životnosti emitovat konstantní barvu světla, neměly by se měnit jeho elektrické vlastnosti (konstantní odpor) a měl by mít velice pomalý úbytek jasu v průběhu životnosti. Seřadíme-li dle kvality země výroby dle používaných čipů, lze říci, že za nejkvalitnější jsou na trhu považovány čipy japonské, dále z USA a Tchaj-wanu a Čína, jako již tradičně, produkuje nejčastěji čipy nízké ceny, ale zároveň i kvality. LED čipy byly na trh uvolňovány v generacích označených čtyřmístnými číselnými kódy, kde dvě dvojice číslic udávají rozměry čipu v milimetrech. V níže uvedené tabulce lze spatřit typy čipů seřazené sestupně dle minimálního měrného světelného výkonu.

SMD LED (module)	Dimensions (mm x mm)	Power (watt)	Flux (lumen)	CRI <sup>[3]</sup> (Ra)	Intensity (candela)	Beam angle (degree)	Heatsink (yes/no)	Efficacy (min) (lm/W)	Efficacy (max) (lm/W)
3030	3.0 x 3.0	0.9	110-120					120	130
8520	8.5 x 2.0	0.5 & 1	55-60	80				110	120
4014	4.0 x 1.4	0.2	22-32	75-85				110	160
3014	3.0 x 1.4	0.1	9 - 12	75-85	2.1-3.5	120	yes	90	120
7020	7.0 x 2.0	0.5 & 1	40-55	75-85				80	110
5736	5.7 x 3.6	0.5	40-55	80	15-18	120	no	80	110
3020	3.0 x 2.0	0.06	5.4		2.5	120	no	80	90
7014	7.0 x 1.4	0.5 & 1	35-50	70-80				70	100
5733	5.7 x 3.3	0.5	35-50	80	15-18	120	no	70	100
3535	3.5 x 3.5	0.5	35-42	75-80				70	84
3528 (aka 1210)	3.5 x 2.8	0.06-0.08	4 - 8	60-70	3	120	no	70	100
2835	2.8 x 3.5	0.2	14-25	75-98	8.4-9.1	120	yes	70	125
5730	5.7 x 3.0	0.5	30-45	75-98	15-18	120	no	60	90
5630	5.6 x 3.0	0.5	30-45	70	18.4	120	no	60	90
5050	5.0 x 5.0	0.24	10-18	60-70	5.1-5.75	120	no	58	75

Jak lze vyčíst z uvedené tabulky<sup>34</sup>, efektivita nejhorších LED čipů (dva sloupce napravo – minimální a maximální efektivita) činí až 50 % efektivitu těch nejlepších, přičemž ty nejhorší jsou dle tabulky uvedené na předchozí stránce srovnatelné s nejlepšími kompaktními zářivkami (ty ale mají zvýšený odběr při rozběhu).

## LED svítidla

V předchozích odstavcích byly popsány důležité vlastnosti pro výběr čipů. Koncový zákazník si však nepotřebuje kupovat čipy, avšak svítidlo jako celek. Zásadním rozdílem LED svítidel vůči zářivkám je fakt, že svítidla mohou, ale také nemusí mít výměnný světelný zdroj. Snadno se tak

34 SMD LED module. Wikipedia.org [online]. 2017 [cit. 2017-04-09]. Dostupné z: [https://en.wikipedia.org/wiki/SMD\\_LED\\_Module](https://en.wikipedia.org/wiki/SMD_LED_Module)

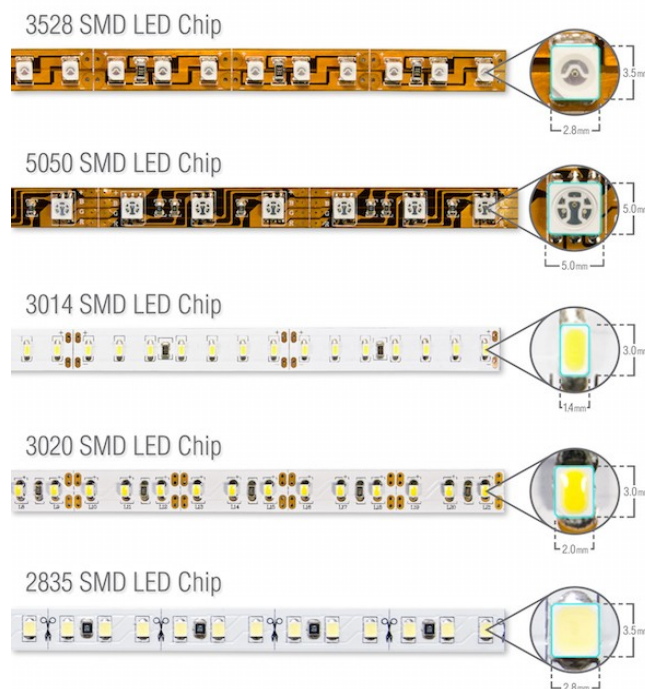
může stát (nejčastěji u plochých svítidel, které je však, na rozdíl od žárovkových a zářivkových provedení, vůbec možno zkonstruovat), že při poruše svítidla je nutné vyměnit celé svítidlo, nikoliv pouze žárovku či zářivku. To může přinést vyšší investice, avšak po několika letech se také může stát, že původní svítidlo se již přestane vyrábět a bude tak nutné vyřešit konstrukční změnu.

Předchozí odstavce o LED čipech byly sepsány primárně proto, že při výběru kompaktních svítidel je z výše uvedených důvodů velmi žádoucí dbát zvýšené pozornosti, a to jednak na druh použitých čipů, také ale na konstrukci svítidla samotného.

Nejčastějším problémem, který limituje životnost svítidel, je špatně navržené chlazení čipů. LED čipy, ostatně jako veškerá polovodičová technika, se špatně snáší s vysokými teplotami (cca.  $> 70\text{ }^{\circ}\text{C}$ ). Vzhledem k negativní teplotně-odporové charakteristice protéká při vyšších teplotách součástkou vyšší proud, což vede ke zvyšování odporových ztrát, přehřívání a následně také destrukci součástky.

V praxi se tak lze u nekvalitních svítidel často setkat např. se situací, kdy přestane svítit polovina LED žárovky. V případě zářivek a žárovek se nikdy nestane, že by přestala svítit polovina zdroje – ten buď funguje nebo nefunguje (popř. má vadný předřadník). U LED modulů ale, vzhledem k jejich konstrukci (velké množství SMD čipů spojených do sério-parallelně zapojených bloků), záleží na elektrickém zapojení svítidla. V případě této události v záruční době je tato závada jednoznačně důvodem k oprávněné reklamaci. Je tak velmi důležité alespoň pohledově zjistit, zda má svítidlo dostatečně veliké tepelně vodivé plochy, kudy bude odvádět nežádoucí teplo od čipů

Některá svítidla na bázi LED mají při připojení přímo na síťové napětí rovněž problém se stroboskopickým efektem. Zda tímto neduhem trpí nebo ne se odvíjí od vnitřního zapojení svítidla. Výrobci levnějších svítidel využívají faktu, že LED čipy jsou vlastně z principu funkce usměrňovače a připojí tak sériově zapojené bloky těchto diod na síťové napětí přímo. Ti lepší pak využijí obě části sinusoidy v síti využitím dvou antiparalelně zapojených bloků (každý pro  $U_{ef} > 230\text{ V}$ ) a místo tepavého světla o frekvenci 50 Hz dostaneme tepavých 100 Hz. Ta nejlepší svítidla pak využívají stabilizovaného napájení za účelem potlačení stroboskopického jevu. Do doby, než jsou světla umístěna a zapojena je tak těžké určit, zda je konkrétní svítidlo náchylné na tento problém. V plošných instalacích lze tento problém eliminovat již v projektu pomocí zapojení tří sad světel, které jsou navzájem prostorově promíchány, přičemž každý set je zapojen na jinou fázi. V důsledku překryvu sinusoid napětí jednotlivých fází je tak dodávka světelného toku zajištěna kontinuálně s minimální pulzací.



Kdy tedy má smysl využít svítidla zářivková, kdy LED a kdy přicházejí ke slovu žárovky?

Zářivková svítidla jsou ekonomicky výhodnější po stránce pořizovacích nákladů, vzhledem k vysoké ceně regulačních předřadníků jsou vhodnější spíše do prostor, kde je zapotřebí světla jen zapínat a vypínat (bez regulace jasu – což vyhovuje ve většině učeben, které lze v tomto případě dokonce prohlásit za dokonalý modelový případ). Zářivky jsou zdroje dokonale plošné, mají chladnější světlo a jejich efektivita je nižší, avšak v případě dražších zářivek srovnatelná s levnějšími LED svítidly. Cena za světelný zdroj o ploše a výkonu zářivky je ve srovnání s LED svítidly příznivější právě pro zářivky.

LED svítidla naleznou uplatnění tam, kde se vyžadují minimální rozměry svítidla, nenápadný design, vysoká efektivita, nízká spotřeba a dlouhá životnost. Barevné podání LED svítidel je mnohem lepší, než v případě zářivek. Vybrat si lze z různých teplot světla, oproti zářivkám nejsou náchylné na zapínání a vypínání, zvládají rovněž pracovat v extrémně nízkých teplotách, které dělají zářivkám problém. K sehnání jsou na trhu nejrůznější kreativní designy, dají se snadno regulovat (nevyžadují předřadníky, startovací napětí, atp.). Zvláště vhodné je jejich využití v tělocvičnách ve stíněných plošných svítidlech jako náhrady za neefektivní a nespolehlivé staré výbojky.

Pozorného čtenáře by jistě napadlo, proč zde autor neuvedl kompaktní úsporné zářivky a výbojky. Odpověď je jednoduchá – kompaktní zářivky jsou principiálně shodné s trubcovými, jen mají vlastní předřadník integrovaný přímo v těle kolem závitu, a výbojky jsou již obecně

spíše na ústupu. Význam mají pouze v aplikacích pro trvalé osvětlení a v aplikacích s požadavkem na extrémně vysoký světelný tok (jako je např. osvětlování stadionů). Výbojky jsou značně náchylné na časté spínání a v prostorách škol mají v nových instalacích pouze marginální uplatnění a průběžně jsou nahrazovány efektivnějšími zdroji.

V případě žárovek je situace velice specifická. Ač se může na první pohled zdát, že s nařízením EU o zákazu prodeje žárovek jakožto světelných zdrojů nastal jejich definitivní konec, je nutné si uvědomit, že žárovky mají jako jediný světelný zdroj koeficient barevného podání na úrovni 100 %, což z nich činí unikátní nástroje např. pro účely zobrazování. Kvalitního osvětlení je nutné docílit žárovkami také u všech točivých pracovních strojů. Vzhledem k vlivu již popisovaného stroboskopického efektu u jiných typů světla je velice vhodné, ne-li přímo nutné, zajistit osvětlení pracovního prostoru stroje (soustruhy v dílnách, vrtačky, brusky, motory, atp.) právě žárovkami. Ty, vzhledem k principu funkce (termoemise fotonů žhaveným vláknem) netrpí – vlákno totiž 100× za sekundu nestihne zchladnout, polarita napětí i frekvence jsou mu jedno a jakmile se žárovka jednou rozehřeje, svítí konstantně pořád.

### **Percepce barvy světla**

Jako doplňkový faktor při výběru svítidel do prostor školy je také vhodné zvážit i vliv osvětlení na lidskou psychiku. Ta je ovlivněna nejen technickými parametry světla jako jsou teplota barev nebo úplnost vyzařovaného spektra, ale i barvami zastoupenými v místnosti. Výše popsané faktory mají totiž prokazatelně vliv na fyziologické a psychologické děje odehrávající se v tělech a myslích žáků a zaměstnanců školy. Tématika výběru barev vhodných pro stimulaci studijního prostředí je však hodna samostatné práce a případným čtenářům, které předchozí zmínka zaujala autor doporučuje přečtení výchozího zdroje.

Jako zajímavé stojí za zmínku zjištění autora zdroje <sup>35</sup>, že studené barvy jsou statisticky více preferovány žáky sekundární školy, zatímco teplé barvy preferují spíše děti v předškolním a nižším školním věku. Pro zachování útulnosti a zároveň stimulaci studijní nálady je dle autora této práce vhodné využít světelné zdroje o teplotách 3500-4000 K.

V úvahu je rovněž vhodné vzít i důsledky přítomnosti zvýšené intenzity modré části spektra:

---

35 GAINES, Kristi S.; CURRY, Zane D. The inclusive classroom: The effects of color on learning and behavior. *Journal of Family & Consumer Sciences Education*, 2011, 29.1: 46-57.

„Není žádným tajemstvím, že kromě epifyzy se na udržení cirkadiálního rytmu podílí také nucleus suprachiasmaticus a retina. Jedním ze zájmů posledního výzkumu bylo vyhodnotit, jak se věkově závislé ztráty čirosti oční čočky a oblasti pupily odráží na "cirkadiálním vidění".

Pouze asi 1 % retinálních gangliových buněk patří mezi fotoreceptory. Přesto toto relativně malé množství buněk hraje zásadní roli v lidské fyziologii a zdraví. Buňky totiž exprimují ftopigment melanopsin (na rozdíl od tyčinek a čípků produkujících rodopsin), který je senzitivní na modré světlo. Modré světlo se na produkci melanopsinu podílí z 53 %, zatímco fototoxické fialové světlo pouze z 15 %. Zmíněné melanopsinové receptory regulují tvorbu hormonu melatoninu a komplexní systém melanopsin–epifyza–melatonin synchronizuje naše vnitřní vnímání času s vnějším časem.

Stárnoucí oko, respektive jeho buněčné elementy, je citlivější na krátkovlnné části světelného spektra. Takové oko pak v rámci své ochrany reaguje úbytkem lipofuscinu v pigmentovém epitelu sítnice a vlastní čočka reaguje vznikem katarakty, čímž se oko brání fototoxickému účinku modrého světla.

Pro srovnání je u desetiletého dítěte až 10× větší cirkadiální vidění než u 95letého důchodce. Proto asi nikoho nepřekvapí, že právě u starších lidí jsou poruchy denního rytmu velmi časté. Jejich důsledkem pak mohou být psychovegetativní poruchy, deprese či poruchy srdečního a krevního oběhu.

Z tohoto důvodu se k léčbě popsaných poruch využívá i tzv. fototerapie. Pro udržení synchronizace fyziologicky nastavených vnitřních hodin s vnějším světem stačí denní osvětlení o intenzitě pouhých 200 luxů. Pro terapii poruch cirkadiálního rytmu je ale zapotřebí osvětlení o intenzitě přesahující 2 000 luxů. Teprve taková intenzita světla dokáže zastavit tvorbu melatoninu v epifyze.“

Pro detailní popis tohoto jevu z pohledu technického doporučuje autor pročtení zbytku bakalářské práce pana Petra Dvořáka z VUT v Brně.<sup>36</sup>

## **Shrnutí**

Světelná technika skrývá obrovský potenciál optimalizací nejen po stránce úspory energií, ale rovněž bylo poukázáno na fakt, že vhodnou volbou osvětlovacích technologií je možné

---

36 DVOŘÁK, Petr. Vliv modrého světla na lidský organismus [online]. Vysoké učení technické v Brně. Fakulta elektrotechniky a komunikačních technologií, 2016 [cit. 2017-04-06]. Dostupné z: <http://hdl.handle.net/11012/60483>. Bakalářská práce. Vysoké učení technické v Brně. Fakulta elektrotechniky a komunikačních technologií. Ústav elektroenergetiky. Vedoucí práce Jaroslav Štěpánek.



dosáhnout zlepšení životnosti světelných zdrojů v daných podmínkách, zvýšení požární a elektrické bezpečnosti budov a v neposledním případě také zvýšení efektivity učebního procesu. Byly zdůrazněny málo známé faktory hrající roli při výběru osvětlení pro účely školního prostředí a popsány kritické body, na které se zaměřit s ohledem na neinformovanost laické veřejnosti, což v tomto případě vedení škol většinou bývá.

### 4.3 Topení a vzduchotechnika

V poslední dekádě je ve spojení s evropskými dotacemi cílenými na ekologii životního prostředí kladen důraz na zlepšení tepelně-izolačních vlastností budov s cílem zamezit zbytečným energetickým ztrátám. Ač jsou tato stavební opatření nepochybně nejdůležitější cestou jak dosáhnout zamýšleného výsledku, cílem této práce je popsat několik doplňkových řešení, jak jejich účinnost ještě dále vylepšit a jak vyřešit potenciální problémy vycházející z podstaty zateplování budov.

Každý člověk si jistě je schopen vybavit několik situací z poslední doby, kdy se při soustředěné práci začal najednou cítit unavený, nevykonný, s upadající pozorností, případně jej začala znenadání bolet hlava. Tyto symptomy jsou příznakem zvýšené koncentrace CO<sub>2</sub> v uzavřeném prostoru, jehož nárůst je vzhledem k nízké rychlosti těžké zaznamenat.<sup>37, 38</sup> Ve škole je tak běžným jevem, že se otevřou okna za účelem větrání. To však přináší několik otázek:

1. Jak poznat, že je nutné vyvětrat?
2. Umíme vůbec větrat?
3. Postačuje otevření pár oken k vyvětrání třídy aktivně pracujících jedinců?
4. Hygiena?

---

37 Větrání škol: problémy vedou k nové vyhlášce. Smart Cities [online]. Praha, 2017 [cit. 2017-04-06]. Dostupné z: <http://www.scmagazine.cz/casopis/01-16/vetrani-skol-problemy-vedou-k-nove-vyhlasce?locale=cs>

38 Hygienické parametry vnitřního prostředí ve třídě. ASB-portal.cz: odborný stavební portál [online]. Praha: Jaga Media, 2016 [cit. 2017-04-06]. Dostupné z: <https://www.asb-portal.cz/tzb/vetrani-a-klimatizace/hygienicke-parametry-vnitriho-prostredi-ve-tride>

## 1. Jak poznat, že je nutné vyvětrat?

Jak poznat, že je nutné vyvětrat je velice složité. Situace ve třídě se odvíjí od několika proměnných:

- objem vzduchu ve třídě – v menších třídách stoupá koncentrace CO<sub>2</sub> rychleji
- výchozí stav při příchodu do třídy – je těžké odhadnout koncentraci CO<sub>2</sub> ve třídě, která byla delší čas zavřená a kde díky tomu již není vysoká vlhkost (mohla projít zdmi, může být třída přetopená, atp.) - významný podíl na odhadu, zda je vzduch „vydýchaný“ má primárně jeho vlhkost
- počet žáků ve třídě – více zdrojů CO<sub>2</sub> → rychlejší nárůst koncentrace
- aktivita žáků – toto se dá zjednodušit na „výkon“ těchto zdrojů CO<sub>2</sub>
- proudění vzduchu ve třídách – ve starých třídách byla montována dřevěná okna, která jednak nebyla tak těsná jako moderní vícevrstvá plastová okna; kromě toho však původní dřevěná okna, pokud jsou stále osazena, bývají do značné míry opotřebovaná a tudíž i netěsná – jsou v nich jsou mezery, kterými volně proudí vzduch a dochází tudíž v omezeném měřítku k samovolné výměně vzduchu v místnosti; v některých třídách (např. laboratoře) bývají rovněž umístěny digestoře nebo ventilační komíny, které tento jev podporují

Větrání je tak založeno primárně na pocitu žáků a zaměstnanců školy a jejich vzájemné komunikaci. Žáci však na tento problém nebývají vůbec připraveni, nejsou zvyklí sledovat vlastní aktivitu a příčiny jejího opadání a je jim to do značné míry jedno. Je tak primárně na učiteli, zda sleduje aktivitu žáků ve třídě a zda je schopen si spojit jejich případnou únavu s koncentrací CO<sub>2</sub> ve třídě.

### Řešení:

Množství CO<sub>2</sub> přítomného v ovzduší v místnosti je možné sledovat prostřednictvím speciálních snímačů, které vyrábí např. firma ABB jako strojek určený pro zapuštění do instalačních krabic různých designových řad. Při překročení limitu displej s hodnotou zčervená a lze využít jeho dvou bezpotenciálových výstupů k automatizaci reakcí – např. lze ovládat automatické otevírání oken nebo spínat ventilaci. Fungovat však může i v samostatném režimu a lidé si mohou

po upozornění snímačem otevřít okna sami. Snímač zobrazuje i teplotu, vlhkost a tlak vzduchu a je možné zablokovat jeho manuální ovládání proti neoprávněným zásahům (např. o přestávkách).

## **2. Umíme vůbec větrat?**

Častým nešvarem je špatný styl větrání. Je nutné si uvědomit, že cílem větrání nemá být snížení teploty v místnosti, ale výměna vydýchaného vzduchu za čerstvý. Z energetického hlediska je nejefektivnější větrání nárazové, prudké, s průvanem, kdy se vzduch v prostoru vymění za co nejkratší okamžik. Vysoká efektivita souvisí úzce s nízkou měrnou tepelnou kapacitou vzduchu a zároveň vysokou měrnou tepelnou kapacitou ostatních předmětů v místnosti a zdiva. Při rychlé výměně vzduchu tak nestihnou předměty s vysokou tepelnou kapacitou zchladnout a opětovné prohřátí místnosti je dílem okamžiku. Pokud však větráme pomalu, např. jen přes ventilace, bude docházet k postupnému ochlazování místnosti a všech objektů uvnitř a na její vytopení následně spotřebujeme mnohem více energie, než by bylo potřeba v prvním uvedeném případě. Ventilací větrání není ani efektivním prostředkem k zajištění celkové výměny vzduchu ve třídě.

Řešení:

Jako vhodné řešení se jeví primárně proškolení zaměstnanců. V případě, že jsou k dispozici finanční zdroje lze přistoupit i k nasazení elektronických regulačních hlavic na ventily radiátorů a magnetických senzorů na okna. Logika zpracování se nabízí taková, že při větrání se topení vypne a nebude tak docházet ke zbytečnému plýtvání energiemi, popř. lze výkon topení pouze snížit. S instalací termohlavic se nabízí i připojení do centrálního systému regulace topení.

## **3. Postačuje otevření pár oken k provětrání třídy aktivně pracujících jedinců?**

Záleží na konstrukci oken i daného prostoru. Jak prokázalo terénní měření zdroje, leckdy je i v případě otevření oken větrání v malých prostorech nevyhovující. Vždy je však nutné pro kvalitní analýzu situace v daném prostoru provést měření přímo na místě za běžných podmínek. Lze však také jít cestou preventivní eliminace problému a přistoupit k řešením navrhovaným níže.

## **Řešení:**

Proškolení zaměstnanců zaměřené na krátké využití všech oken pro větrání. Vynucení této politiky lze zajistit instalací řízené ventilace.

## **4. Hygiena**

Problémy s větráním přináší dva zásadní hygienické problémy:

*„ (zvýšená koncentrace CO<sub>2</sub>) způsobuje nižší soustředěnost, nižší psychické výkony, neklid, při dlouhodobém pobytu ve znečištěném prostředí pak bolest hlavy (častá příčina ranní bolesti hlavy, neboť dle měření velká část českých ložnic není dostatečně větraná). Důsledkem je i snížená imunita, a tím pochopitelně i zvýšená nemocnost. Nedostatečné větrání se projeví i neodváděním mikrobů, a tím intenzivnějším šířením kapénkové infekce.“<sup>24</sup>*

## **Řešení:**

Řešením výhradně tohoto problému může být instalace čističky vzduchu, která průchozí vzduch desinfikuje UV zářením nebo vysokonapětovou ionizací. Toto řešení se však nezabývá problémy s unikajícím teplem a zvýšenou koncentrací CO<sub>2</sub>.

Jako teoreticky nejvýhodnější se jeví využití komplexního řešení všech uvedených problémů:

- nucené větrání s rekuperací, prachovými filtry a UV desinfekcí vzduchu
- průběžná pomalá nucená ventilace bez průvanu
- spínání rychlé ventilace v jednotlivých místnostech již při podlimitních hodnotách CO<sub>2</sub>
- magnetické snímače na oknech v kombinaci s tepelnými čidly v místnosti a elektronickými regulačními hlavicemi
- ekonomické úspory dynamickým řízením vytápění reagujícím na změny teploty
- centrální integrované řešení vytápění

Pro zajištění největších možných úspor energetických i ekonomických je vhodné kombinovat řešení s kogeneračními jednotkami, popř. tepelnými čerpadly a v případě více budov v kampusu je vhodné, s přihlédnutím k místním specifikům, zdroj tepla centralizovat. Jako vždy je však nutné koordinovat přípravy řešení s odborníky a přizpůsobit jej charakteru a specifikům dané lokality. Tak jako u všech technických projektů je vhodné konzultovat jejich řešení s více stranami (a optimálně nezávislým odborníkem), vzájemně jejich navrhovaná řešení konfrontovat. Tím lze efektivně zjistit a odstranit slabiny jednotlivých návrhů ještě před jejich realizací, případně některé návrhy včas vyřadit.

#### **4.4 Informační systémy školy**

Škola je ze své podstaty organizace pracující s informacemi. Informací jakéhokoliv druhu v rámci každé školy není málo a je nutné se v nich neztratit. Nedílnou součástí škol se tak od přelomu tisíciletí začaly stávat i informační systémy různých druhů, které umožňují zefektivnění školních procesů skrze třídění informací a efektivní nakládání s nimi. V níže uvedených odstavcích jsou uvedeny ty nejvýznamnější informační systémy (s výjimkou účetních a právních), které nebývají úplně běžné a mohou pomoci školám se zlepšením procesů či eliminací zbytečných problémů.

##### **Fenomén za zkratkou WWW**

Asi nejdůležitějším informačním systémem z pohledu člověka nezapojeného přímo do dění školy je školní web. Webová prezentace slouží nejen k vlastní propagaci a komunikaci školy s veřejností, ale i jako informační a komunikační prostředek uvnitř školy samotné. Web každé školy navštěvuje několik základních skupin návštěvníků: stávající žáci, jejich rodiče, zájemci o studium, veřejnost, čas od času i zřizovatel a v neposlední řadě také učitelský sbor školy.

Každý web by měl být perfektně přehledný, nacházení informací by mělo být pro návštěvníka velice intuitivní, ovládacích prvků by nemělo být v zájmu zachování přehlednosti přehršel. Z tohoto důvodu se z pohledu autora osvědčily dva základní přístupy k členění webu a to buď dle tématu nebo dle cílové skupiny návštěvníků.

Design webové stránky bude specifický dle zaměření dané školy a preferencí zadavatelů tvorby webu. Měl by zohledňovat specifika dané organizace – rozdílnou grafickou podobu bude

mít církevní ZŠ, prestižní gymnázium, strojní, umělecko-průmyslová nebo zemědělská škola. Každá škola by měla (i s přihlédnutím k ekonomicky efektivním metodám vlastní propagace) mít vlastní profesionální jednotný grafický styl, který se projeví nejen na webových stránkách, ale i na hlavičkovém papíru, v jednotných e-mailových podpisech nebo v prezentačním vzoru. K tomuto bodu je vhodné poznamenat, že je žádoucí vynutit jeho používání vnitřním předpisem a že jeho implementaci by měl mít na starost jediný člověk, při jehož výběru by měl brát zřetel na dlouhodobou spolupráci (profesionálně propagovaná škola má lepší image – digitální grafika v současnosti vládne i sociálním médiím, což je kanál pro komunikaci s mládeží). Rovněž je vhodné ošetřit právní hledisko související s autorskými právy – vzhledem k potenciálním dopadům případných sporů mezi grafikem a školou je žádoucí si hned od začátku ujasnit, aby se vlastníkem díla stala škola. To samé platí, vzhledem k povaze díla, i pro webové stránky.

Úvodní stránka by měla obsahovat obsah, který prvotního návštěvníka zaujme, pravidelného efektivně informuje o novinkách a cíleně jdoucího za specifickým obsahem bez nutnosti hledání rychle nasměruje na požadovanou stránku. Je rovněž nutno vzít v úvahu, že v rámci vlastní propagace vyžadují umístění svého loga i zřizovatel nebo sponzoři školy. Je proto vhodné v rámci úvodní stránky webu vybrat reprezentativní a nerušivé umístění i pro tyto prvky.

Nedílnou součástí kvalitní webové prezentace by měly být primárně detailní kontakty. Je žádoucí uvést základní kontaktní údaje o škole (oficiální název, adresa, telefon na sekretariát) přímo na úvodní stránku (např. do bočního panelu či zápatí). Dále se jeví jako velmi vhodné zřízení extra stránky s detailními kontakty a informacemi o škole, která může obsahovat např. i rozšířené adresní informace, oficiální centrální telefonní a e-mailový kontakt, IČO, DIČ, IZO školy nebo ID datové schránky (existenci faxu v roce 2017 nepředpokládáme).

Další vhodnou obsahovou položkou jsou kontakty na jednotlivé učitele, popř. další zaměstnance. Stránku s kontakty na jednotlivé zaměstnance lze rovněž pojmout různými způsoby. V případě menších škol, kde jsou pouze jedna nebo dvě sborovny, lze kontakty na zaměstnance pojmout jako kontakt na sborovnu a pedagogický sbor uvádějí na jiné stránce, včetně aprobací. Některé školy volí cestu uvedení tabulky s e-mailem a telefonem (případně i mobilním), někde je možné si jméno pedagoga rozkliknout a objeví se jeho osobní medailonek i s fotografií. Záleží vždy na domluvě zodpovědných pracovníků, pro kterou variantu se rozhodnou.

Školní web je vhodné tvořit strukturovaně. Ač bylo v době psaní práce v módě vyrábět jednostránkové bezodkazové prezentační weby (např. zde: <http://service.ihned.cz/smartycity/>), tato struktura se nejeví ve větším množství odkazů jako přehledná. Školní weby jsou ze své

podstaty obsahově náročné a neslouží jen k prezentaci tématu či vysvětlování specifické problematiky, ale umožňují uživateli složitou hierarchickou navigaci. Jako vhodné se jeví klasické hierarchické členění, optimálně s využitím vertikálně vysouvacích horizontálních menu. Moderní web by měl být rovněž responzivní, tzn. že se dynamicky přizpůsobí obrazovce, na které je zobrazován. Optimalizace obsahu pro mobilní zařízení (a připojení) by rovněž měla být samozřejmostí.

Web by měl mít k dispozici redakční systém pro uživatelsky přívětivé rozhraní pro editaci obsahu. Je také velice důležité držet na paměti, že sebelepší web nemůže fungovat a vypadat dobře, pokud tvůrce jeho obsahu nerozumí pravidlům pro tvorbu webu, pro práci s jeho rozhraním, základní typografii a základům počítačové bezpečnosti.

Níže lze nalézt inspiraci v podobě výčtu vhodných obsahových prvků běžně užívaných na školních webech. Ne všechny prvky jsou využitelné univerzálně pro všechny školy, tento seznam však může posloužit k načerpání inspirace:

- vlastní propagace – zprávy a reportáže z médií, speciální vybavení školy, osvědčení, úspěchy žáků, historie školy, virtuální prohlídky (např. přes Google Street View), projekty realizované na škole (např. Erasmus+, ESF, aj.), příprava na jazykové zkoušky,
- informace o možnostech stravování a ubytování pro žáky i veřejnost
- rozpis plánovaných akcí na školní rok
- rozvrh hodin a plánované změny v rozvrhu
- odkazy na další interní systémy (např. web systému Bakaláři, e-learningové systémy, e-mailové rozhraní, systém pro správu účtu v jídelně, knihovnický portál, atd.)
- foto a videogalerie (např. prostřednictvím odkazů na oficiální školní kanály služeb Instagram a Youtube)
- úřední deska, dokumenty školy
- výroční a inspekční zprávy
- složení školské rady, žákovský parlament
- partneři školy v oblasti školství a také komerčního sektoru
- informace o dostupných možnostech poradenství

- informace pro uchazeče – nabízené obory a zaměření (včetně jednotlivých ŠVP), podmínky přijímacího řízení
- informace pro budoucí absolventy – informace o možnostech dalšího studia, popř. práce
- informace pro veřejnost – kalendář veřejných akcí školy, možnosti pronájmu prostor školy, kurzy, případně např. výstupy ze školní meteorostanice, atp.

Pro správnou funkci webu je nutné zajistit i kvalitní prostředí pro jeho běh. Weby pro svou funkci využívají protokolů HTTP a HTTPS (Hypertext transfer protocol (+secure)). Tyto protokoly slouží k nešifrovanému a šifrovanému přenosu dat k vykreslování dané webové stránky. Fungování webu je založeno na transportní architektuře klient-server. Jako klient funguje jakékoliv obligátně využívané zařízení k prohlížení webových stránek s tzv. webovým prohlížečem – počítač, telefon, tablet, atp. Klient pošle požadavek na webový server (první krok může být např. zadání adresy do prohlížeče), ten jej zpracuje a pošle klientovi. Klient následně pošle další požadavek (např. po kliknutí uživatele na odkaz) a situace se opakuje. Do procesu je samozřejmě zapojeno mnohem více protokolů, než je HTTP (DNS(SEC), TLS, protokoly nižších vrstev, atd.), pro vysvětlení základního principu je však ponechme stranou.

Server je velmi důležitou částí systému, která má výrazný vliv na rychlost a spolehlivost fungování webu. Lze jej představit jako zařízení připojené do internetu s nainstalovanou aplikací, která dynamicky zpracovává požadavky uživatelů na webový obsah a který překládá strojově zpracovatelný kód do lidsky přívětivé podoby. Server může být provozován buď přímo školou (která většinou již nějakým serverem disponuje – slouží i pro jiné účely) nebo poskytovatelem hostingových služeb. Výhodou vlastního hostingu je využití existujících prostředků, kterými škola již disponuje, dokonalá kontrola nad nasazenou technologií a možnost využití detailních serverově orientovaných statistik. Nevýhodou vlastního hostingu je složitá obrana proti webovým útokům, vysoké nároky na kvalifikaci správce systémů, zálohování systémů, konektivitu serveru a výkon síťových prvků, přes které webový provoz prochází. Záleží na zvážení školy, zda bude ochotna platit za bezpečnou, avšak drahou infrastrukturu poskytovanou provozovatelem hostingu nebo zda raději bude řešit starosti spojené s nutností pravidelné údržby systémů. Pokud není kladen důraz na bezpečnost, spolehlivost a chybovou odolnost využívaných technologií, může se snadno stát, že se škola bude brzy potýkat s bezpečnostními problémy.



## **Intranet a interní massmédia**

Pro účely vnitřní komunikace lze ve škole zřídit i výhradně interní webové stránky sloužící např. jako rozhraní infokiosků. To jsou místa, kde lze rychle a přehledně dopátrat omezený set informací potřebný pouze při fyzické přítomnosti ve škole. Tento systém tak může uživatelům umožňovat např. tisk z flash disků prostřednictvím předplaceného kreditu (např. přes kód nebo identifikační kartu), poskytovat rychlé informace o jinde neveřejných rozvrzích učitelů, viditelně zveřejňovat výstrahy (ztráty a nálezy, výpadky sítě, atp.), popř. umožnit přístup k mediálním archivům.

Ve školství se lze setkat i s jednosměrnými informačními kanály, nejčastěji v podobě velkých informačních obrazovek, které na rozdíl od infokiosků nenabízejí uživateli interaktivitu. Tyto obrazovky je pak možné využívat např. k zobrazování předdefinované obrazové smyčky nebo třeba k hromadnému zobrazování videostreamu. Výhodou těchto obrazovek je, že lze snadno centrálně ovládat jejich obsah bez nutnosti násobně zatěžovat síť – lze využít multicast streamu ze serveru ke klientským zařízením. V současné době se jeví jako vyhovující a zároveň ekonomické řešení využití obrazovek s podporou HDMI, které lze nastavit na automatické zapnutí a vypnutí v předdefinovanou dobu, popř. které se dokáží vypnout při nepřítomnosti videosignálu. Autor navrhuje v případě zájmu školy o tuto technologii využití televizních obrazovek LCD (nikoliv plazmy kvůli vypalování pixelů při zobrazování statických snímků) v kombinaci s Google Chromecast Ultra zapojeného do gigabitové sítě a softwarem Greenscreen (k nalezení na GitHubu), jenž dokáže streamovat předdefinované webové stránky, které je již jednoduché spravovat.

## **Školní management**

Informační systémy školního managementu slouží k práci s daty přímo účastnými v procesu výuky. Mezi jejich základní funkce se řadí např. správa identit žáků, evidence jejich absence a klasifikace, tvorba a editace rozvrhů žáků, pedagogů i učeben, správa přijímacích řízení, úvazků pedagogů a komunikace se žáky a rodiči. Nejznámějšími systémy používanými v ČR jsou Bakaláři, Škola Online a SAS.

## **GSuite**

Autor již čtvrtým rokem ve škole aktivně spravuje systém GSuite for Education. Jedná se o balík cloudových aplikací poskytovaný firmou Google vzdělávacím institucím zcela bezúplatně. V tomto balíku je zahrnuto mnoho vysoce užitečných aplikací. Jako velice vhodné pro prostředí českého školství se jeví nasazení e-mailového systému s uživatelským rozhraním shodným se službou G-Mail (případně nově je podporována i služba Inbox), které mnozí učitelé již důvěrně znají a není tak nutné je přeškolovat na proprietární školní systém. V rámci GSuite je škole poskytnuto určité množství uživatelských účtů (s jejich počty nebývá problém – co si škola řekne, to dostane), přičemž každému účtu je přiděleno neomezené datové úložiště v rámci služby Disk (Google Drive). Toto úložiště je společné i dalším aplikacím, jako je právě E-mail, Dokumenty, Tabulky, Prezentace, a jiným. Zásadní výhodou GSuite for Education je však existence Administrátorské konzole (Admin console), což je místo, ke je možné vytvářet uživatele, jejich skupiny, těm přiřazovat různé politiky pro správu a nebo jim povolovat či zakazovat jednotlivé aplikace sady GSuite. Skrze tento balík je pak možné provozovat např. perfektně spolehlivý e-mailový systém školy, úložiště osobních dat jednotlivých uživatelů (ať už žáků nebo učitelů), online editor dokumentů s možností živé kooperace na jednom dokumentu, hromadné kooperativní e-mailové schránky, fóra, jediný oficiální školní Youtube kanál, správu organizace v Mapách Google, edukační portál Classroom a další věci, to vše s intuitivním rozhraním, výbornými možnostmi přizpůsobení.

## **Infrastrukturní služby**

Velice důležité informační systémy jsou rovněž ty, které nejdou vidět. Jelikož většina škol funguje na platformě Windows, nelze zde neuvést systém Active Directory. Tento systém slouží jako katalog pro správu síťových identit, evidenci počítačů, tiskáren a aplikaci politik pro správu síťových prostředků. K tomuto katalogu lze přistupovat prostřednictvím dalších služeb distribuovaných v rámci systému Windows Server jako k autentizačnímu serveru RADIUS, který může zprostředkovávat ověření uživatelského jména a hesla např. pro přístup k WiFi sítím školy. Rovněž je AD možné využít jako LDAP server, kdy je možné načítat katalog identit pro další systémy (např. VoIP telefony nebo dále popsany server pro řízení tisku). Hlavní funkcí je však aplikace bezpečnostních a konfiguračních politik pro klientské stanice Windows, prostřednictvím kterých lze hromadně např. instalovat nebo odinstalovat software, změnit nastavení plochy nebo zakázat uživatelům přístup k jiným, než povoleným složkám v síti. Možnosti využití tohoto systému jsou velmi široké a pro školství se stal prakticky nezbytností.

Další z infrastrukturních služeb jsou systémy pro řízení bezpečnosti sítě. Pod tím si lze představit např. služby VPN zajišťující uživatelům možnost vzdáleného připojení do vnitřní sítě školy, řízení obsahu dostupného zevnitř sítě (blokování aplikací nebo webů) nebo klasický firewall. Ač o těchto systémech většina lidí nemá ani ponětí, jsou jedny z nejdůležitějších pro datový provoz v organizaci a měla by jim být věnována patřičná odborná péče i z důvodu zajištění jejich bezpečnosti. Nejlépe lze tento fakt demonstrovat na případu dat uvolněných v rámci projektu Vault7, kdy server Wikileaks uvolnil dne 7. 3. 2017 obrovské množství utajovaných dat, ve kterých byly popsány metody využívané bezpečnostními agenturami USA, jak prolomit zabezpečení běžně komerčně využívaných síťových prvků. Ač tyto zprávy zůstaly médií nepovšimnuty, v odborných kruzích se v následujících dnech strhlo pozdvižení (které bylo vcelku očekávané), když se mezi zveřejněnými daty objevila informace, že pomocí určitých nástrojů lze získat kontrolu nad síťovými prvky renomovaných výrobců jako je Mikrotik, Ubiquiti Networks, Cisco, Solaris, zasaženy byly také produkty firmy Microsoft.<sup>39,40</sup> V měsíci od vypuštění těchto dat došlo u mnoha síťových produktů k vydání aktualizovaného firmwaru, který dle e-mailových notifikací výrobců (což už samo o sobě nebývá zvykem, šlo tedy o důležité opravy) řešil bezpečnostní opatření. Mikrotik tak učinil dva dny od vypuštění dat z Vault 7 (9. 3. 2017)<sup>41</sup>, Ubiquiti Networks 20. 3. 2017 (doložitelné e-mailem) a Cisco vydalo bezpečnostní doporučení v této věci dne 17. 3. 2017.<sup>42</sup>

## **Služby pro tiskový management**

Ve školách je většinou obrovský zdroj potenciálních úspor skryt ve financování tiskových služeb. Vzhledem k náročnosti tématu na odborné znalosti je běžným jevem ve školách nákup levných tiskáren s drahým provozem, popř. omezení přístupu pedagogů k tiskovým službám.

Jelikož tištěné digitální materiály se staly v moderní škole běžnou součástí výuky a jelikož veřejné finance nebolí zaměstnance, ale jen zřizovatele a vedení, zaměstnanci školy si leckdy ve škole tisknou i materiály pro domácí potřebu. Je tak běžným jevem, že se školy snaží šetřit a zavádějí opatření pro monitorování a limitování tisku. Systémy, které toto mají na starost,

---

39 Wikileaks Unveils 'Vault 7': "The Largest Ever Publication Of Confidential CIA Documents"; Another Snowden Emerges. Ron Paul - Liberty report [online]. 2017 [cit. 2017-04-06]. Dostupné z:

<http://www.ronpaullibertyreport.com/archives/wikileaks-unveils-vault-7-the-largest-ever-publication-of-confidential-cia-documents-another-snowden-emerges>

40 Vault7 - Home. Wikileaks [online]. 2017 [cit. 2017-04-06]. Dostupné z: <https://wikileaks.org/ciav7p1/>

41 All current and historical changelogs. Mikrotik.com [online]. Riga, LV, 2017 [cit. 2017-04-06]. Dostupné z: <https://mikrotik.com/download/changelogs>

42 The Wikileaks Vault 7 Leak – What We Know So Far. Cisco.com [online]. 2017 [cit. 2017-04-06]. Dostupné z: <http://blogs.cisco.com/security/the-wikileaks-vault-7-leak-what-we-know-so-far>

vytvoří virtuální tiskárnu, na níž se následně odesílají tiskové úlohy. Uživatel při tisku zadává své identifikační údaje (jméno a heslo, popř. přiloží kartu) a dle nastavení platného pro konkrétního uživatele je vybrána tiskárna. Tu si buď může zvolit přímo uživatel a tisknou přímo, popř. může odeslat úlohu na společnou tiskárnu (nebo společnou tiskovou frontu), následně k ní přijít a přiložením karty tisk spustit (v případě společné fronty na kterékoliv tiskárně pracující s danou frontou). Vyšší náklady na pořízení systému, zařízení s ním kompatibilních a zavedení do praxe mají většinou rychlou návratnost (řádově 1-3 roky) v podobě ušetřených celkových ročních nákladů na spotřební materiál a servis tiskáren. Jako vhodný se v případě nemožnosti investic jeví pronájem tiskových zařízení od specializovaných firem. Nejznámější systémy pro tiskový management v ČR jsou SafeQ, MyQ a Papercut NG.

Opomíjenou možností na školách je zřízení veřejné tiskárny / kopírky pro žáky. Je zřízení tiskových služeb pro žáky zbytečným luxusem nebo je toto řešení na školách z pohledu přínosu pro vzdělávání žáků žádoucí?

Na základních školách lze s jistotou tvrdit, že je podobný systém zbytečný. Vzhledem k zacílení vzdělávacích programů základních škol primárně na rozvoj základních kompetencí žáků lze konstatovat, že na základních školách nejsou tiskové služby pro žáky potřebné. Navíc, pokud je již tato služba z pohledu žáků potřebná, mohou si ji zajistit s rodiči ve městě (rozhodně to nebývá na denním pořádku).

Situace se však rapidně mění na školách středních, kde je po žácích mnohem častěji vyžadována samostatná kreativní práce a kde zadávání seminárních prací není výjimkou. Ne všichni žáci disponují tiskárnou doma a časté návštěvy polygrafického centra by zvláště pro dojíždějící žáky mohly představovat narušení časového rozvrhu dne. Zde je vhodné umístit (např. formou pronájmu) černobílou síťovou multifunkci formátu A3, k ní umístit tiskový počítač a využít přístupových karet nebo čipů ke správě uživatelského konta. Toto konto je pak možné dobíjet např. hotovostní platbou na sekretariátu školy nebo lze zřídit (např. pro odlehčení vytíženého sekretariátu) webové rozhraní pro dobíjení konta prostřednictvím platebních karet.

Co se týká tiskáren, naprosto nevyhovující řešení je nákup malých tiskáren do majetku školy a jejich umístění do každé kanceláře. Ač je toto řešení pohodlné, rozhodně není ekonomicky rentabilní. Úplně nejhorší je umístit do kabinetu barevnou tiskárnu a tisknout na ní 95 % tisků černobíle. Barevná tiskárna (laserová – o ekonomice inkoustů se nemá ani cenu bavit) obsahuje místo jednoho fotoválce a odolného transferového válce rovnou fotoválce čtyři a k nim ještě problémový transferový pás. Pořízení barevné tiskárny se tak s koncem životnosti optické

jednotky prodraží, protože nestačí koupit levný fotoválec, ale celou drahou optickou jednotku. Ekonomičtější pak bývá pořízení nové tiskárny...

Řešením je co největší možná míra centralizace tisku a výhodné pořízení či lépe pronájem enterprise class tiskárny. Velká zařízení určená pro velké objemy tisku totiž dokáží tisknout za mnohem nižší náklady, než zařízení malá. Místo tisku za 1,50 až 2,50,- Kč za stránku se tak lze dostat až k 0,20,- Kč za stránku. Krom toho se lze s firmami domluvit na operativním pronájmu, kdy při dostatečném objemu tisku se platí jen cena za stránku v předem dohodnuté ceně a starost o servis tiskáren je problémem pronajímatele. Tisk tak již nemusí přinášet zvýšené náklady a je možné jej využívat i ve větším objemu. Navíc je toto řešení ekologičtější, jelikož pracujeme s tiskárnami s řádově delší životností, a komfortnější pro uživatele, jelikož větší tiskárna umožní uživateli větší funkcionalitu a lepší produktivitu.

## 4.5 Systémová integrace

V předchozích řádcích jsme si popsali řadu opatření, které lze operativně přijmout pro zajištění úspor a efektivity procesů v organizaci. Neméně důležité je však nezapomenout na zajištění jednoduchosti správy a spolehlivosti všech systémů. Z pohledu systémového administrátora je pro tyto účely nejvhodnější zavést integrační systém, který bude potřebné administrativní úlohy sdružovat pod jediný programový celek.

Zásadním problémem, který je nutné vyřešit při realizaci integrace systémů je ale fakt, že každý systém je unikátní a že zakoupitelné či volně stažitelné ready-to-deploy integrační systémy nejsou a z podstaty rozdílů mezi školskými systémy jednotlivých států ani nemohou být univerzální a napojitelné na všechny systémy, kterých se škola rozhodla z nejrůznějších důvodů využít. Ty systémy, které se za univerzální prohlašují, jsou také cíleny spíše na větší trhy a je důležité si uvědomit, že Česká Republika není pro vývojáře softwarových řešení příliš lukrativním cílovým trhem. Může se tak snadno stát, že si škola, v případě, že se rozhodne podobný systém realizovat, bude muset systém naprogramovat od základu, popř. dotvořit softwarové moduly pro umožnění komunikace s danými nepodporovanými systémy.

Jako vhodný základ pro integraci se jeví kombinace backendu, který v podobě systémové služby dokáže načítat data z monitorovacího systému (jako je např. již zmiňovaný Zabbix), CCTV, EZS, EVS a EPS, zpracovávat je do unifikovaného formátu ve vlastní databázi;

a frontendu v podobě dynamického webového rozhraní (využívající např. moderní AJAX) pro integraci a jednotnou správu. Výhodou je správa prostřednictvím webového prohlížeče bez nutnosti instalace specializovaných aplikací – tento systém tak lze prostřednictvím protokolů nižších vrstev zabezpečeně provozovat odkudkoliv. Jako vhodné se jeví tuto aplikaci zpřístupnit přes webové rozhraní, které bude čerpat podkladová data z databáze (např. otevřené a spolehlivé MySQL nebo jeho modernější sesterské MariaDB). Rovněž pokládám za vhodné tento systém síťově zpřístupnit pouze z vnitřní sítě školy a případně přes VPN, má-li dostatečnou konektivitu a výpočetní výkon na zařízení zprostředkovávající službu VPN (levnější routery nemusejí na šifrování videa dostačovat).

Uživatelské rozhraní integračního systému musí být uživatelsky přívětivé, tzn. okamžitě na první pohled přehledné, musí mít intuitivně rozmístěné a identifikovatelné ovládací prvky (optimálně grafické symboly), dostatečnou velikost (nutno vzít v potaz i velká rozlišení na menších obrazovkách a lidi s horším viděním) a daná funkce musí být přístupná optimálně jediným kliknutím. Rovněž je vhodné implementovat funkce pro úsporu datových toků (manuální obnovení, kamery pouze na vyžádání, atp.).

V případě integrace systémů EVS (kontrola přístupu) + CCTV (kamery) + EZS (alarm) + EPS (požární systém) navrhuje autor využít pro objekt dlaždicově uspořádaný systém s živým náhledem podkladových map objektu po jednotlivých patrech (1 patro = 1 volně zvětšovatelná a přesunovatelná dlaždice) s nastavitelnými segmenty, do nich přiřazenými funkčními prvky a barevným rozlišením jejich stavu. Po rozkliknutí daného prvku by se měl zobrazit jeho stav (EZS: stav detektoru, EVS: poslední průchody s možností otevření detailní historie, CCTV: aktuální obraz z kamery s možností otevření videoarchivu, atp.) a umožnit interaktivně uživateli další práci s ním. Systém by měl rovněž umožnit práci více uživatelů s rozdílnými právy. Dvě základní úrovně by měly obsahovat práva 1) pouze pro čtení a 2) pro editaci map a prvků systému. Uživatelé by pak měli mít možnost přistupovat k různým subsystémům a pro jednotlivé prvky by měla existovat možnost přiřazení operačních práv pro jednotlivé uživatele.

Do integračního systému lze potenciálně zakomponovat i jiné systémy, než bylo uvedeno v předchozím odstavci. V úvahu tak připadají např. aktivní síťové prvky (dostupnost a vytížení switchů a routerů), ovládání energetických rozvodů (světla, silnoproudé okruhy, topení), řízení centrální ventilace v daných částech objektu a jiné specifické systémy (za vše lze uvést příklad v podobě dálkového hromadného odstavení zařízení v učebnách od sítě, central stop pro elektřinu a plyn, atd.).

Možnosti integračních systémů jsou v době softwarově definovaného řízení zařízení skrze síť TCP/IP omezené pouze kreativitou jejich tvůrců. Je dobré mít na paměti, že kvalitně propracovaný systém může vydržet na škole fungovat dlouhá léta. Stejně tak je však dobré myslet i na komunikační bezpečnost těchto systémů a uvědomit si, že každé zařízení a systém zapojený do datové sítě je napadnutelný, jen si nemusíme být prozatím vědomi způsobu. Je tak např. žádoucí zadat tvůrci, popř. nezávislému odborníkovi, jednou za čas bezpečnostní audit nejen tohoto systému, ale i celé sítě a nechat si prověřit její potenciální slabá místa. Podobný audit nemusí být úplně levný, dokáže však zabránit podstatně dražším škodám. I z tohoto důvodu je vhodné vyvinutý systém nepovažovat za jednou provždy hotový, ale např. jednou ročně nechat tvůrce zkontrolovat jeho chyby a ve smlouvě předem ošetřit škody způsobené jejich zanedbáním. Dokážeme tak předejít výrazným problémům.

## **5 Co přinese budoucnost?**

V předchozích kapitolách byly rozebrány možnosti aplikace systémových řešení v době psaní této práce. Tato kapitola má naopak za cíl shrnout technologie, se kterými se školy budou moci setkat v blízké budoucnosti, analyzovat hypotetické scénáře rozvoje a navrhnout možnosti reakce škol na technologický rozvoj.

### **Internet of Things**

Ač je toto „buzzword“ hojně využíváno médií a technologickými firmami již několik let, prakticky se tento pojem používá prakticky pro cokoliv. Co však všechny tyto zdroje mají společné je technologický myšlenkový směr sjednocování strojů a systémů do jednotných celků skrze datové sítě.

Hlavní idea fenoménu Internet of Things (dále jen IoT) spočívá v integraci dosud samostatných systémů v oblastech běžného života. V praxi se tento technologický myšlenkový směr projevuje implementací síťových rozhraní např. do ledniček, praček, kuchyňských spotřebičů, žárovek, automobilů, rozvojem chytrých silnoproudých domovních instalací, atd.

Fenomén IoT rozsáhle pracuje s myšlenkou síťování nejen prostřednictvím již existujících metalických sítí Ethernet a bezdrátových sítí WiFi, ale hlavně koketuje s vizí všudypřítomných bezdrátových sítí dvou typů. První typ představují již existující a testované

WAN sítě páté generace umožňující zařízením a uživatelům využívat vysokorychlostní konektivity v řádech gigabit za sekundu. Tyto by měly nahradit dnes využívané LTE. Druhým typem jsou poprvé nasazované sítě LPWAN (low power WAN).

Koncept sítí LPWAN přináší uživatelům možnost využívat pomalé datové přenosy v delších intervalech na velké vzdálenosti při zajištění minimální spotřeby. LPWAN sítě procházejí v době psaní práce v celé Evropě dynamickým vývojem, kdy se teprve vyjasňuje, který z technologických konceptů různých výrobců se na trhu prosadí a uchytí. V ČR jsou majoritně využívány dvě technologie – LoRa (provozovatele České Radiokomunikace) a SigFox (T-Mobile). Obě technologie pokrývají krajská města, LoRa je však dostupná na mnohem větší části území naší republiky.<sup>43</sup>

Školství se fenomén IoT může dotýkat primárně v následujících oblastech:

- chytré řízení vytápění v budovách
  - jak již bylo popsáno dříve, řešení již existují, avšak nejsou ve školství využívána – není o ně zájem a přinášejí vyšší prvotní investice, ale i provozní úspory
- projektory, tabule, tiskárny, světla, vše připojené do datových sítí pro ovládání, vzdálenou diagnostiku a konfiguraci a automatizaci hlášení potřeby údržbových prací
  - systémy pro správu budov již taktéž existují, ale školství o nich prakticky neví
- cloudové environmentální hlásiče přes LPWAN
  - detektory bezústřednových alarmů a EPS připojené přímo do cloudu, uživatel si bude moci vybrat aplikaci, kterou pro tyto systémy využije
  - potenciál amatérské spolupráce s výzkumnými institucemi v oblasti výzkumu počasí, stavu půdy, seismologie, atp. – státní školy jsou perfektními subjekty pro spolupráci s výzkumnými institucemi
- aplikace ideologie smart cities do škol
  - inteligentní parkovací systémy pro větší kampusy
  - chytré osvětlení (dynamicky řízený jas LED zdrojů) v kombinaci s environmentálními detektory (teplota, vlhkost, hluk, znečištění, ...)

---

43 Mapa pokrytí. IoT portál: brána do světa internetu věcí [online]. 2017 [cit. 2017-04-06]. Dostupné z: <https://www.iot-portal.cz/mapa-pokryti/>



- dynamicky řízený svoz odpadu (chytré popelnice)
- chemické a radiační detektory pro bezpečnostní aplikace
- chytré energetické sítě – vzdálené odečty spotřeby a provozních parametrů v síti, dynamické řízení tarifů dle aktuální situace, automatizace detekce poruch
- implementace NFC jako náhrady identifikačních karet a čipů nebo platebních karet

### **Změny v konektivě škol**

Vzhledem ke změnám ve společnosti souvisejícím s extenzivním rozvojem mobility a preference využívání vlastních zařízení jak žáky, tak zaměstnanci školy je nutné brát v potaz i bezpečnostní rizika související s připojováním potenciálně nezabezpečených nebo přímo nebezpečných zařízení do jedné sítě. V budoucnosti se tak školy nevyhnou investicím do zvýšení síťové bezpečnosti přímo související s principy technologické ideologie známé pod zkratkou BYOD (bring your own device). Ve školách bude nutné nastavit politiky pro žáky a zaměstnance, zavést opatření pro filtraci obsahu a ochránit všechny před škodlivými internetovými zdroji.

Problémy lze do budoucna očekávat právě v oblasti filtrování obsahu, kdy tradiční metody filtrování přestávají s rozvíjejícími se snahami o šifrování veškerých datových toků být efektivní. Ač je možné prostřednictvím proxy serveru poskytnout uživateli vlastní certifikát a spojení tak dešifrovat a zašifrovat následně znova po analýze, toto řešení je vysoce problematické již nyní s nástupem technologie HSTS, která podvrhnutí certifikátu efektivně brání. Uživatel se tak k požadovanému obsahu vůbec nedostane. Rozmach tak zažijí inteligentní technologie filtrování založené např. na hybridní (automatické s lidskou korekcí) klasifikaci webů dle URL (čehož uživatel využije prostřednictvím výrobcem tvořené a udržované databáze), identifikaci zero-day hrozeb skrze jejich prvotní zachycení a analýzu na honeypotech a následném rozšíření prostřednictvím updatů nebo dynamických dotazů na cloud, analýze využívání portů danými programy a klienty a porovnáváním provozu se známými podezřelými vzorci.

V oblasti konektivity škol do sítě Internet lze počítat s exponenciálním nárůstem požadavků na propustnost sítí, což úzce souvisí s rostoucími nároky na výkon jednotlivých síťových prvků a celkovou konektivitu škol. Tyto nároky budou způsobeny jednak plynulým technologickým přechodem k zařízením pro záznam a přehrávání médií ve vyšším rozlišení,

jednak přechodem ke cloudově orientovaným službám při současné eliminaci lokálních serverových služeb.

Celkovou konektivitu škol bude možné navyšovat několika způsoby. Jednak je žádoucí komunikovat s městy a žádat při realizaci výkopových prací v okolí školy vybudování optických tras do páteřních datacenter (kde je to možné). V tomto ohledu je možné využít služeb národní sítě pro vzdělávací instituce – CESNETu. Pro školy, které nemají přehled o možnostech vzájemné spolupráce tato organizace doporučuje obrátit se s požadavkem o informace na příslušný e-mail (v době psaní práce [sluzby@cesnet.cz](mailto:sluzby@cesnet.cz)). Jedná se primárně o služby poskytování vysokorychlostního datového připojení, virtuálních serverů nebo AAA (authentication, authorization, allowance) služeb v rámci mezinárodní sítě eduroam. Dalším způsobem připojení, který se aktuálně teprve utváří, by mělo být připojení právě přes již zmíněné 5G sítě, které by měly umět poskytnout dostatečné rychlosti i tam, kde připojení vysokorychlostní optikou nebude z různých důvodů uskutečnitelné. Diskutovány jsou v odborných kruzích čím dál častěji i vizionářské plány do delší budoucnosti na bezdrátové broadbandové pokrytí buď celé planety prostřednictvím satelitů na nízkých oběžných drahách (analogie GPS sítě) nebo plošné pokrytí daných oblastí autonomními retranslačními drony nebo dokonce balóny.

Dále je nutné počítat s plynulým přechodem z adresace IPv4 na IPv6 a postupně sítě při jejich budování raději kapacitně a výkonově předdimenzovat a klást důraz na jejich kompatibilitu právě s IPv6 a souvisejícími protokoly. Tuto funkcionalitu nemusíme využívat do doby, než to bude nutné (např. vyžadováno poskytovateli nebo provozovateli služeb), je však důležité, aby prvky související protokoly již uměly. V opačném případě by školu čekala vysoká nárazová investice, protože by prvky byly nevyhovující.

## **Změny ve výuce**

Školství se z pohledu autora bude muset rovněž přizpůsobit rostoucím nárokům na informační gramotnost žáků. S nástupem konceptu Průmyslu 4.0 se změní požadavky trhu práce na kvalifikaci pracovníků. Na žáky budou tudíž kladeny mnohem větší nároky na specializaci v oblasti informačních systémů. Na co žáci ve školách v současnosti nejsou připravováni vůbec a co je do budoucna vysoce perspektivní oblast je např. 3D tisk, práce s drony, programování mikrokontrolerů a praktické základy automatizace. S čím se lze ve výuce setkat již nyní je např. výuka práce s elektronickými zabezpečovacími systémy. Tyto systémy jsou však vyučovány

nikoliv plošně, ale prakticky výhradně na odborných školách. Ač budou velice důležité, tyto oblasti vyžadují vyšší investice do materiálního vybavení, jednak kladou nároky na odbornost vyučujících, kteří se budou muset kontinuálně vzdělávat, optimálně jezdit na konference a sdílet zkušenosti prostřednictvím různých vzdělávacích platforem. Práce s výše uvedenými technologiemi je také velice náročná a za dvě vyučovací jednotky nelze kvalitně obsáhnout. Z tohoto důvodu bude nutné ICT věnovat i lepší hodinové dotace.

To s sebou přináší i nutnost legislativních změn – jako velmi žádoucí se jeví zkrácení reakčních časů legislativy a metodik na změny ve společnosti, zlepšení objemu a cílenosti financování škol v oblasti IT zdrojů tak, aby na tyto technologie dosáhly všechny školy plošně. Rovněž se jeví jako velice žádoucí zavedení kvalitního financování pro odborné vzdělávání pedagogů vyučujících ICT, které je, na rozdíl např. od vzdělávání učitelů českého jazyka (bez urážky), mnohem dražší, jelikož vyžaduje úzce odborníky úzce specializované na dané téma. V neposlední řadě je rovněž vhodné zlepšit financování nepedagogických pracovníků, aby si školy vůbec mohly odborníky dovolit.

# APLIKAČNÍ ČÁST

Aplikační část je věnována kazuistice rozvoje bezpečnostních systémů v prostředí školních budov. Pro názornější ilustraci bude využito přímé srovnání situace na škole základní a střední, z čehož vyplynou rozdílné nároky menších a středních organizací na požadavky zabezpečení. Z důvodu ochrany fyzické a datové bezpečnosti popisovaných škol nejsou jejich jména v textu konkrétně uvedena, jsou však známa vedoucímu práce a komisi.

Školy byla oslovena prostřednictvím e-mailů směřovaných ředitelům, kdy po udělení souhlasu z jejich strany byly předjednány schůzky realizované v průběhu měsíce dubna 2017 přímo na půdě škol. Zástupcům vedení a místním koordinátorům ICT byly položeny otázky týkající se všech systémů popsaných v teoretické části práce a autor si s těmito zástupci prošel školní budovy. Nad uvedenými otázkami byla vedena diskuze, kdy se autor snažil zjistit doplňující informace, zajít do detailů a získat názory a detailní připomínky všech zúčastněných osob k dané problematice. Zhodnocení výsledků výzkumu následuje formou diskuse nad jednotlivými tématy a uvedením hodnotících připomínek autora s cílem vyvodit závěry využitelné v praxi třetími stranami.

## ***I. Obecné poznatky***

S vedením obou organizací byly nejprve prodiskutovány záležitosti týkající se obecných údajů o nich a dále oblasti managementu a financování ICT.

Nejprve byly školy dotázány na celkový počet žáků, kteří školu navštěvují. Tento parametr může posloužit k vytvoření obrázku o celkové velikosti zkoumaných organizací:

- ZŠ: 245 žáků – malá základní škola, bez spádové oblasti, menší nároky, více flexibilní
- SŠ: 700 žáků (610 SŠ + 90 VOŠ) – velká střední škola krajského významu

Oslovená základní škola sídlí v jediné budově patřící zřizovateli a ničím zvláštním po organizační stránce se nevymyká.

Dotazovaná střední škola sídlí v kampusovém areálu, který sdružuje více budov, krom primární historické i dvě přilehlé pro odborné praktické vzdělávání. Škola v době psaní práce

poskytuje kromě středoškolských vzdělávacích programů i jeden program pro vyšší odborné vzdělávání. Škola má vlastní internát cca. 300 metrů od hlavního kampusu a detašované pracoviště v jiné části města (pozůstatek po sloučení s jinou školou), které využívá spíše okrajově z důvodu odtržení lokality od hlavního areálu. Využívá se proto prakticky výhradně pro výuku VOŠ. Obě dotazované školy sídlí v historických budovách zbudovaných ve 20. letech 20. století.

Další dotaz směřoval na vyjádření k průměrné roční výši provozních výdajů školy:

- ZŠ: 2,5 mil. Kč
- SŠ: 8,6 mil. Kč

Tyto údaje posloužily především k výpočtu procentuálního zastoupení investic do hardware a software (viz oddíl klientské stanice níže).

## **II. ICT management**

### **Personální zodpovědnost**

Na základní škole se o ICT stará interní zaměstnanec, který je zároveň na této škole pedagogem vyučujícím informatiku, fyziku a matematiku. Tento pedagog je za tuto práci odměňován snížením počtu hodin z úvazku (dle nařízení vlády 75/2005 §4 odst. c) o 3 hodiny týdně, navíc je za svou činnost ředitelem školy ohodnocen odpovídající finanční odměnou. Do jeho kompetencí spadá správa a údržba školních počítačů (počty viz níže), tiskáren, školního serveru (1 fyzický, na něm 1 host a 1 virtuální server), webových stránek školy a síťových prvků ve škole fungujících. Správce má v případě potřeby k dispozici na výpomoc školníka, pro odbornější úkoly, jako je rekonfigurace virtualizace, centrálního firewallu nebo výběr a konfigurace prvků bezdrátových sítí, také externí partnery. Vedení školy je se současným stavem správy sítě spokojeno a zastává názor, že prostředky vynaložené na správu ICT jsou z dlouhodobého hlediska vynakládány efektivně a nepocit'uje výrazná omezení brzdící rozvoj ICT.

Škola správci poskytuje vyšší příspěvky i s ohledem na vyšší náklady na samostatné vzdělávání a vychází mu vstříc s požadavky na uvolnění za tímto účelem. Jak však vyplynulo z dalšího rozhovoru, žádná odborná certifikační školení zaměřená na metodiku správy ICT

v organizaci, popř. školení zabývající se výukou odborných kvalifikací pro systémy hromadné správy tento správce neabsolvoval.

Na zkoumané střední škole se o správu ICT stará externí živnostník v kombinaci s interním zaměstnancem školy. Odměňování funguje na bázi smlouvy mezi školou a živnostníkem, který skrze vlastní účetnictví paušálně odměňuje daného učitele. Učitel je rovněž odpovídajícím způsobem ohodnocen vedením v rámci osobního ohodnocení k platu. Živnostník má rovněž vzhledem k objemu práce nasmlouvány vlastní specialisty (a specialistky) na konkrétní oblasti ICT. Vzhledem k velikosti školy, vysokým nárokům na odbornost při realizaci složitějších projektů a souhrnně většímu objemu práce jsou pracovní úkony rozděleny mezi jednotlivé pracovníky. Interní učitel má na starosti běžnou údržbu techniky, řešení méně odborných požadavků na on-site podporu uživatelů, řešení akutních problémů, vedení licenční politiky školy a evidenci počítačů. Slouží rovněž jako spojka mezi odbornějšími pracovníky (kteří mají tuto práci pouze jako přivýdělek) a školou. Další pracovník se specializuje na správu serverové a síťové infrastruktury a souvisejících služeb včetně bezdrátových sítí, přístupového systému a platformy pro výdej stravy ve školní jídelně, správu software a definici standardů konfigurace klientských stanic, správu identit, řízení obsahu a monitoring systémů. Další pracovník je orientován na vývoj, správu a zabezpečení webových aplikací (škola provozuje vlastní server, na němž běží více webových služeb – oficiální web, rezervační portál pro externí partnery, environmentální portál pro veřejnost, systém Bakaláři, portál pro správu knihovny, Moodle, monitoring, datové úložiště, meteorologická služba, ad.), další specialista se stará o chod portálu školní knihovny a poslední zainteresovaný člověk se stará o výpomoc v oblasti pozáručního servisu porouchané elektroniky a rovněž zajišťuje drobné pomocné práce v této oblasti (pájení konektorů, lištování kabeláže, atp.). Veškeré vzdělávání personálu je výhradně v režii živnostníka a zaměstnanců samotných. V případě potřeby jsou práce na předběžné vyžádání kooperovány se školníkem a údržbářem. Vedení školy je se stavem správy sítě z personálního hlediska spokojeno. Výhrady však padly v oblasti efektivity vynakládání prostředků na tisk, kde je výhradním limitem nejasnost rozhodování zřizovatele, který škole přikazuje vykonávat objednávky skrze krajský portál a rovněž zakazuje uzavírat smlouvy na odběr služeb v délce trvání přesahující jeden rok. Tato omezení vedou v tomto konkrétním případě k nemožnosti efektivně srazit vysoké náklady na tisk při zachování stejného rozsahu služeb pro zaměstnance prostřednictvím outsourcingu tiskových služeb.

Obě školy mají dále navázanu spolupráci s externími subjekty v oblasti správy telefonních systémů a zabezpečovacích zařízení (detaily viz níže, pro každý systém specialisté).

**Komentář:** Na výše uvedených datech lze dobře pozorovat rozdíl mezi časovými a personálními nároky na správu menší a rozlehlejší organizace. Je patrné, že oslovené školy se snaží zajistit chod organizace s nejnižšími možnými náklady. Kromě modelu externích subjektů v kooperaci s interními zaměstnanci je často možné setkat se i se scénářem snažícím se o úplnou eliminaci potřeby externích subjektů prostřednictvím zaměstnání odborníka na plný úvazek. Této situaci se však oslovená střední škola snažila vyhnout. Jednak je to pro ni bezpochyby pohodlnější z hlediska administrativního, ale tím nejdůležitějším důvodem je přísné rozdělení finančních zdrojů, ve kterých se školám dlouhodobě nedostává financí na platy nepedagogického personálu. Škola si tak může dovolit ufinancovat lepší služby z rozpočtu provozního, který vyplácí zřizovatel, nikoliv MŠMT. Prakticky pravidlem však je, že organizace preferují mít v záloze člověka na místě, který může zasáhnout v případě akutního problému, alespoň pro řešení s odborníky prostřednictvím telefonu.

### **Plánování údržby a investic**

Obě školy mají zpracován dlouhodobý plán ICT, podle něhož se řídí jejich další rozvoj v této oblasti. Ten je důležitý pro stanovení jasných cílů, souvisejících metod, procesů a kontrolních ukazatelů, jak těchto cílů škola dosáhne a jak si ověří jejich dosažení. Obě školy uvedly, že tento plán dynamicky aktualizují dle aktuálních potřeb. Rovněž vedení na obou školách souhlasilo se stanoviskem, že v posledních pěti letech museli rapidně změnit plány v této oblasti nebo odložit jejich realizaci v důsledku změn vyžadovaných zřizovatelem či jinými nadřízenými orgány. Plán ICT může rovněž posloužit jako kvalitní zdroj informací pro plánování investic do údržby a obnovy technických zařízení a ušetřit prostřednictvím konsolidace shodných investic nemalé finanční prostředky. Pro tento účel je však nutno stanovit intervaly plánované životnosti zařízení s ohledem na podmínky jejich používání (jak často se používají, životnost udávaná výrobcem, možnosti údržby po skončení prodeje, atp.). Školy byly dotázány, zda mají naplánovány plánovanou cyklickou obnovu hardwaru. Ani jedna ze škol tuto metodiku nevyužívá a problémová zařízení mění až když je to potřeba. Obě školy se po vysvětlení metodiky prediktivního plánování rozhodly, že popsání opatření zavedou.

**Komentář:** Plán rozvoje ICT se rovněž jeví jako vhodné udržovat i ve firmách, popř. si jej dobře promyslet již před stavbou nebo rekonstrukcí jakéhokoliv objektu. Je totiž velmi důležité dbát

na přípravu tras datových a energetických sítí pro zamýšlené, ale i doposud neznámé systémy, které je možno nasadit v budoucnosti. Prakticky může tato příprava mít podobu nachystání kabelových průchodek, rozvodů strukturované kabeláže (vhodné nachystat pod omítku kabelové průchodky, teprve do nich uložit SKS – možno po čase vyměnit bez potřeby zednických prací) a silových zásuvek nebo rozbočovacích krabic na strategická místa stavby. Ze zkušeností autora s dozorováním rekonstrukcí elektroinstalace je nemálo častým případem, že na tyto velice důležité věci projektanti stavby nebo rekonstrukce vůbec nemyslí. Přitom datová kabeláž, která se dnes do zdí natáhne, zde bude s vysokou pravděpodobností sloužit ještě dalších pár desetiletí.

Přístup „řeš co se pokazí“ pramení primárně z nevědomosti a neznalosti pracovníků zúčastněných v rozhodovacím procesu. Jednak vede k vysoké míře morálního zastarávání, dále k problémům způsobeným prodlevami mezi poruchou zařízení a jeho nahrazením za nové, jednak ale také k vyšším cenám za výměnu těchto zařízení – pokud by byly investice plánovaně konsolidovány, např. výměna projektorů v osmi třídách najednou, a byly na tuto akci předem alokovány finanční zdroje, bylo by možné dosáhnout nižších cen a to např. prostřednictvím velkoobchodní objednávky s patřičnou množstevní slevou, popř. lze také nákupy realizovat v období plošně nižších cen (u spotřební elektroniky často v létě nebo v povánočním čase) nebo v období silnější koruny, jelikož spotřební elektronika se nejčastěji velkoobchodně obchoduje za dolary či eura. Rovněž lze vyčkat na cílené produktové promoakce distributorů. Souhrnně tak lze prediktivním plánováním získat čas potřebný pro uskutečnění výhodného nákupu či vypsání výběrového řízení, které je např. právě pro školy povinností při zadávání nadlimitních zakázek. Aby však systém fungoval spolehlivě, je vhodné počítat ve všech výpočtech s kratší životností a ve všech investicích s předdimenzováním rozpočtu. Odložit plánovanou investici lze vždy a za služby lze vždy jednoduše zaplatit méně, než více. Jako vhodné se rovněž jeví nenakupovat nový materiál na sklad, ale ihned jej uvádět do provozu, aby se případné vady projevíly včas. Záruka a lhůty na vrácení dodaného zboží běží i ve chvíli, kdy leží ještě zabalené na skladě.

### **III. Datová infrastruktura**

Pozn.: Tato část se zaměřuje na zhodnocení technologií potřebných k existenci moderních bezpečnostních systémů a výzkum existujících predispozic k jejich budování ve zkoumaných organizacích.



Zkoumané školy byly v obou případech vybaveny strukturovaným kabelážním systémem. Zřízení strukturovaných kabelážních systémů mělo ale na zkoumaných školách jiné příčiny. Zatím co na škole základní byla prvotní síťová infrastruktura, na kterou se vývojově navazovalo, vybudována v rámci projektu INDOŠ, střední škola budovala infrastrukturu ve spolupráci s místním poskytovatelem internetového připojení již dříve. SŠ tak měla k dispozici připojení metalickou kabeláží cat. 5e, přičemž tato kabeláž byla vybudována díky kooperaci školy s poskytovatelem prostřednictvím barterového obchodu, kdy škola hradila pouze reálně spotřebovaný materiál a poskytovateli bylo umožněno na škole vybudovat vlastní retranslační stanici pro přilehlou městskou část.

Obě školy disponují strukturovanou kabeláží v kategoriích 5e a 6, přičemž v kategorii 6 byly v případě ZŠ zhotoveny pouze 2 páteřní linky od hlavního rozvaděče k serveru, v případě SŠ pak všechny páteřní linky v hlavní budově. ZŠ využívá tři rozvaděčů v jediné budově s celkovým počtem využitelných portů pohybujícím se okolo jednoho sta, SŠ využívá na hlavní budově taktéž tři rozvaděče, avšak s počtem využitelných datových portů blížícím se šesti stům. Krom nich ale disponuje ještě dalšími rozvaděči, po jednom na dvou přilehlých budovách odborného výcviku, internátě a detašovaném pracovišti.

Následuje zevrubný popis datové infrastruktury základní školy. První rozvaděč je v kanceláři školy, kde je rovněž ukončena přívodní optická linka poskytovatele připojení do Internetu. Tento rozvaděč je zde umístěn z historických důvodů, jelikož na stejném místě je ukončena i telefonní přípojka, přes kterou byl Internet provozován v době, kdy do něj byla škola poprvé připojena právě v rámci projektu INDOŠ. Je zde umístěn 28-portový switch TP-Link TL-SL3428, jehož hlavním úkolem je poskytovat vnitřní konektivitu v rámci třetiny budovy (nijak extra strukturovaně, šlo o první školou realizovanou etapu rekonstrukce elektroinstalace, vše v rámci ní bylo svedeno do tohoto rozvaděče). Dále je v tomto rozvaděči umístěn převodník optické linky (SM 9/125) na standardní metalickou, o propustnosti 100 Mbps. O patro výše, v počítačové učebně, je umístěn rozvaděč druhý, hlavní, v němž je umístěn hlavní router, routerboard Mikrotik RB450G, dále 52-portový switch TP-Link TL-SL3452 a do něhož vedou z prvního rozvaděče dva páteřní kabely kategorie 5e. První slouží na propojení mezi převodníkem optiky a rovněž hlavním routerem (WAN-eth1), druhý na spoj hlavního routeru se switchem v dolním rozvaděči (LAN-eth2). Zbytek portů slouží k připojení počítačové učebny. Část nejvyššího patra (4 třídy) je bez vybudované strukturované kabeláže, toto patro dosud neprošlo rekonstrukcí plánovanou na následující 2 roky. SK je nahrazena bezdrátovou sítí z nižšího patra. Do routeru, který nabízí 1 WAN a 4 LAN porty dále vedou linky z rozvaděče

ve sborovně, kde je umístěn další 28-portový switch (TL-SL3428; LAN-eth3) a ze serveru, který má v zamčeném skladu postavenou uzamykatelnou skříň ve formě ocelové regálové konstrukce a perforovaného plechu pro zajištění ventilace. Všechny switche podporují členění do virtuálních sítí VLAN dle 802.1q, což je na škole aktivně využíváno k rozčlenění počítačů na čtyři základní podsítě a to na počítače kabinetní (včetně tiskáren), počítače ve třídách, subnet pro servery a poslední podsít' je vyhrazena počítačové učebně. Každý ze switchů nabízí vždy dva metalické gigabitové porty, z čehož jeden je využit jako přívodní (v módu trunk – nese více virtuálních sítí skrze tagované rámce). Druhý port je vždy využit pro počítač s největšími nároky na datovou propustnost do zbytku sítě. Největší roli toto hraje v počítačové učebně, kde je takto připojen učitel'ský počítač, který zpracovává velké datové toky generované softwarem pro řízení učebny (iTALC) na ostatních PC v učebně. Zbytek portů má rychlost 100 Mbps.

ZŠ je v době psaní této práce připojena do sítě Internet prostřednictvím optického kabelu. Toto připojení má však na rok 2017 (kdy je domácnostem za 500 korun měsíčně s DPH poskytováno připojení o rychlosti 100/100 Mbps) a lokalitu nedaleko komunikačních uzlů národního významu katastrofickou rychlost 5/5 Mbps (down/up). Toto připojení je problematické i ve výuce ICT, kdy žáci vyhledávající obrázky efektivně zahltí celou linku do Internetu. Škola byla doporučena revize smluv s poskytovatelem, načež se ukázalo, že tato snaha zde již byla, avšak poskytovatel zneužívá svého monopolního postavení v dané lokalitě a účtuje škole až nesmyslné vysoké částky. Škola si údaje nepřála zveřejnit, avšak oproti zkoumané SŠ s nasmlouvanými desetinásobnými rychlostmi šlo o několikanásobnou částku. Škole bylo doporučeno zahájit jednání s konkurenčním poskytovatelem připojení o možnosti přivedení nové optické linky.

Adresaci v síti zajišťuje DHCP server běžící na hlavním routeru, stejně tak slouží jako odlehčovací DNS server. V provozu je i služba DNS na serveru, zde však slouží pouze pro účely systému Active Directory. Služby pro filtrování škodlivého obsahu škola nevyužívá, vše je v kompetenci dozorcujícího pedagoga a vlastní zařízení žáci do školní sítě připojena mít nemohou.

V provozu je rovněž VPN přes protokol PPTP (původně nasazeno kvůli jednoduchosti připojení). Využívána je tato služba pouze správcem sítě. Vzhledem k nízké bezpečnosti protokolu je v plánu na letní prázdniny 2017 migrace na OpenVPN.

Všechny aktivní prvky sítě v současnosti využívané v této ZŠ jsou v době psaní této práce staré 1,5 roku a byly vyměněny najednou. Škola uvedla, že upgrade firmware síťových prvků

provádí jednou ročně a že s ohledem na velikost a nastavená pravidla neprovádí bezpečnostní audity sítě.

ZŠ disponuje tři roky starým školním entry-level serverem Dell T110 II vybaveným čtyřjádrovým CPU Intel Xeon E3-1220 a 16 GB RAM DDR3 s ECC na frekvenci 1333 MHz (dva páry různých modulů – dodatečně doplněno). Úložiště je zajištěno dvěma 1TB SAS disky připojenými prostřednictvím přídatného řadiče Dell PERC H200. Na tomto serveru je nainstalován OS Microsoft Windows Server 2008 jako hostitelský OS pro technologii HyperV, na té je následně virtualizován druhý server se stejným OS sloužící jako doménový řadič. Na hostitelském serveru je nainstalován taktéž server webový a poštovní Exchange server. Celý server (oba logické) se jednou za den zálohují na konstantně připojený externí disk (s externím napájením). Server není hlídán automatickým monitoringem, na hostitelském serveru ale běží software Dell OpenManage System Administrator, který umožňuje správci (krom jiného) manuálně kontrolovat stav všech hardwarových systémů fyzického serveru. Ten správce zkontroluje cca. jednou za dva týdny až měsíc. Server je rovněž vybaven čipem Baseboard Management Controller (Dell BMC) umožňujícím vzdálené ovládání napájení serveru pomocí protokolu IPMI a samostatného koprocesoru na základní desce, který při přítomnosti napájecího napětí zprostředkovává síťovou komunikaci a ovládání napájení serveru i ve vypnutém stavu. Údržba software serveru probíhá cca. čtyřikrát ročně, údržba hardware jednou ročně.

Na dotaz, zda by škola využila služeb externích bezpečnostních auditorů pro identifikaci problémů, které nemusí být na první pohled zjevné a které jsou potenciálními rizikovými místy pro útok na školu zněla odpověď vedení, že ano. Zároveň však dodali, že o podobných zvycích na jiných školách nikdy neslyšeli a že nepovažují školu za vhodný cíl útoku.

Na otázku, zda má škola nastaveny kontrolní mechanismy pro ověření výsledků práce lidí zodpovědných za stav ICT padla jasná odpověď, a to, že ne a že je kooperace mezi kolegy založena výhradně na vzájemné důvěře.

Vzhledem k účasti školy na projektu INDOŠ autora zajímal i pohled zúčastněných osob na jeho realizaci. Všichni se shodli na faktu, že tento projekt byl souhrnně pro školy velmi přínosný, a to z několika důvodů – jednak nastartoval rozvoj výpočetní techniky ve školách a povědomí o nutnosti tuto oblast ve školství aktivně řešit, dále proto, že poskytl školám základní síťovou infrastrukturu, která byla později rozšiřována, ale hlavně projekt poskytl pedagogům prostřednictvím realizovaných školení znalosti potřebné pro aktivní práci s počítači, jejich začleněním do výuky a poskytl jim informace o existujícím výukovém software. Souhrn těchto faktorů vnímalo vedení školy jako velmi přínosný. Rovněž však zdůraznili, že tento projekt šlo

realizovat i lépe, tzn. že nemuselo dojít k jeho vytunelování, že počet dodaných počítačů nebyl valný, že vybudovaná síť nebyla bez dalších investic použitelná pro jiný účel, než offline výuku, že počítače byly již v době dodání morálně zastaralé a po dvou letech je okamžitě vyměnili a že konektivita školy byla slabá. Poslední bod však již vedení jako problém nevidělo, jelikož šlo o počátky internetové konektivity ve většině škol a školy většinou postupem času samy řešily přechod na nové technologie.

**Komentář:** Na této síti je primární výhodou její stabilita, předimenzovaná propustnost a flexibilita. Síť byla budována s ohledem na co nejlepší poměr cena / výkon při současném zvážení jejího pouze špičkově náročného vytížení (přihlašování žáků do učebny). Síť budoval autor ve spolupráci s Mgr. Vilémem Lukášem v době konání své pedagogické praxe v roce 2015. Primárním impulzem pro rekonstrukci této sítě byly časté výpadky a problémy s fungování software pro řízení učebny, obojí způsobené nestabilitou použitých síťových prvků. Ty byly v době rekonstrukce již zastaralé a výkonově nedostačující, navíc síť v učebně (ale i jinde) byla vyřešena problematicky – byl zde evidentní bottleneck – 7 počítačů se dělilo o jedinou 100Mbps linku a při přihlašování na server, kdy síť využívala tzv. „cestovní profily“ (kdy se při každém přihlášení stahovaly na počítač ze serveru velké objemy dat) byly na pár minut nepoužitelné. Taktéž na nich nefungoval software pro řízení učebny, ten navíc dělal problémy i na jiných PC v učebně. Vedení se na základě zjištěných problémů vyjádřilo, že ač peněz na tuto investici nemá tolik, budou rádi, když se to vyřeší a to jednou provždy a kvalitně. Byly proto po konzultaci vybrány levnější, avšak dobře spravovatelné switche s vysokou propustností (datasheet uvádí 12,8 Gbps a 9,5 Mpps pro TL-SL3428 a 17,6 Gbps a 13,1 Mpps pro TL-SL3452) a ochranami proti zahlcení, byly nataženy nové linky z rozvaděče k počítačům v učebně, síť v učebně byla pro zvýšení stability a bezpečnosti oddělena do vlastní virtuální sítě, ze které byl přístup pouze na server a do Internetu a byly odstraněny veškeré přebytečné prvky v této síti (malé switche, centrální firewall na serveru, zastaralý software pro řízení obsahu).

Využitý router od Mikrotiku je složitější na konfiguraci, za tehdejší pořizovací cenu okolo 3000,- Kč s DPH však nebylo možné koupit výkonnější a lépe nastavitelný router. Ač postrádá inteligentní funkce umožňující uživateli využívat různých moderních vychytávek, jako je např. filtrování provozu dle kategorií na bázi cloudové služby, bohatě pro školní použití postačuje a poskytuje škola do budoucna velkou výkonovou rezervu a jistotu podpory jeho firmware ze strany výrobce (RouterOS je univerzální pro většinu zařízení od Mikrotiku, jen bývá jinak zkompileován). Složitost jeho nastavení je navíc vykoupena obrovskými možnostmi jeho

*konfigurace – administrátorovi umožní detailní konfiguraci i na nízkých vrstvách modelu ISO/OSI. Router navíc nabízí gigabitové porty, které lze v organizaci této velikosti využít právě pro centralizované propojení jednotlivých segmentů prostřednictvím dobře nastavitelného integrovaného switch čipu. V případě potřeby je možné routery dokonce zapojit do režimu HA (high availability) prostřednictvím protokolu VRRP, kdy lze router logicky virtualizovat na fyzickém clusteru a v případě poruchy jednoho fyzického routeru funguje spojení stále dál (což ale samozřejmě neřeší např. chyby ve firmwaru). Router rovněž podporuje různé služby VPN, řízení toku nebo L7 firewall (na sedmé vrstvě velmi složitý na konfiguraci, reálně použitelný je do třetí vrstvy).*

*Škole bylo na základě zjištěných informací doporučeno zvýšit bezpečnost sítě prostřednictvím častějších kontrol aktualizací firmware síťových prvků a jednou ročně detailně analyzovat možná rizika vyplývající z provozu sítě. To se týká primárně hlavního routeru, který je skrze veřejnou IP adresu vystaven do Internetu.*

Sít' větší SŠ je oproti výše popsanému řešení značně složitější a její realizace a správa nákladnější. Díky metalické kabeláži, která již v době běhu projektu INDOŠ škole technicky umožnila využívat připojení až do rychlosti 30 Mbps, se škole dříve oproti jiným otevřely rozsáhlé možnosti dalšího technologického rozvoje. I proto se tento projekt školy zcela vyhnul. Ač tato škola měla společně se všemi klienty za retranslační stanicí sdílenou konektivitu do metropolitní sítě až do výše 100 Mbps, tzn. že mohla využívat této rychlosti k přenosům v rámci města, rychlosti připojení do Internetu se postupně navyšovaly s rozvojem externí konektivity poskytovatele a postupnými úpravami smluv s poskytovatelem připojení. V roce 2016 byla v součinnosti poskytovatele připojení s dělníky pracujícími na poslední etapě rekonstrukce elektroinstalace vyměněna přívodní metalická linka s opakovacím switchem za jednoduchý osmivláknový optický kabel (SM 9/125), který byl ukončen v hlavní serverovně školy a na sousedním objektu (cizí organizace). Optická trasa byla následně propojena přímo do oblastního optického rozvaděče a odtud páteří sítě do metropolitního exchange centra. Sousední objekt je připojen až zpětně přes switch poskytovatele v serverovně školy a to z důvodu zajištění maximální možné propustnosti pro SŠ, na které je stále umístěn retranslátor. Pokrytí nákladů na výměnu kabelové trasy ve výši 10 tis. Kč uhradili z poloviny jak škola, tak poskytovatel. Rychlost připojení k internetu se tak v rámci hlavního kampusu navýšila na 50/50 Mbps se špičkovou propustností až 100/100 Mbps (špičky do pěti sekund). V současnosti škola disponuje v serverovně fyzickým rozhraním umožňujícím v rámci metropolitní sítě kombinovanou konektivitu v řádech stovek gigabitů za sekundu. Je tak vcelku jisté,

že v následujících několika desetiletích nebude z pohledu školy nutné vybudovanou linku měnit. Co bude v budoucnu pro navýšení rychlostí potřeba měnit jsou pouze aktivní prvky. Největší limit představuje v současnosti na výměnu jednoduchý a levný switch v majetku poskytovatele připojení, který umožňuje dosáhnout rychlostí do 100 Mbps. Aktivní prvky v majetku školy jsou už nyní dimenzovány na teoretické maximální rychlosti (při započítání pravděpodobnosti výskytu různých velikostí paketů dle statistiky na centrálním prvku sítě) okolo 450 Mbps. Ač jsou ve škole páteřní linky spojeny gigabitovou sítí, tato hodnota vychází z výpočetního výkonu hlavního routeru (taktéž Mikrotik RB450G). Ten je však již nyní možné za pořizovací cenu okolo 3300,- Kč s DPH nahradit výkonnějším modelem RB850Gx2, který nabízí, v závislosti na scénáři, dvoj- až trojnásobný směrovací výkon a hardwarovou akceleraci šifrování AES128, na což RB450G v případě výraznějšího využití šifrované VPN trpí výkonovými propady (šifrování je výpočetně náročná úloha a je-li přenechána hlavnímu procesoru, rapidně se snižuje propustnost systému). Tento model zajišťuje kompletní řízení provozu na jednoduché, ale na propustnost náročnější síti školního internátu, rovněž zajišťuje šifrované tunelované spojení mezi internátem a hlavní budovou (pro účely managementu infrastruktury, monitoringu a správy dvou učitelských a tří veřejných žákovských PC v rámci školní domény). Školní internát je rovněž připojen optickým kabelem, dokonce stejného poskytovatele, taktéž zde má poskytovatel síťový uzel a rychlost připojení činí 50/30 Mbps (down/up). Spojení na hlavní budovu školy je uskutečněno v rámci jediného mezikroku metropolitní sítě, má proto rychlost 100/100 Mbps (limitovanou jen koncovými switchi poskytovatele). Poslední připojený areál, detašované pracoviště školy, je připojeno metalickým přívodem a ekonomickým tarifem 10/5 Mbps (down/up). Zde je však jen wifi router a repeater pro studovnu a dvě přilehlé třídy.

Infrastruktura SŠ je vzhledem k množství a objemům datových toků nejen směrem od klientů do Internetu, ale i od klientů na 10 využívaných serverů, popř. mezi klienty samotnými, náročná na výpočetní výkon využitých prvků. Přenechat směrování v této síti jedinému routeru by bylo technicky velmi náročné, škola proto vsadila na odlehčovací mechanismus, kdy všechny datové toky uvnitř sítě směřuje prostřednictvím L3 switche Cisco SG500-28. Teprve je-li paket určen pro neznámý rozsah nebo rozsah hlavního routeru (tj. jedině routeru samotnému), je tento paket přeposlán na něj a zde je vykonán překlad adres do Internetu. Routing a vnitřní firewalling (řízení přístupu uživatelů mezi segmenty sítě) probíhá výhradně na hardwarově akcelerovaném switchi pro umožnění rychlé komunikace mezi klienty bez zbytečných proluk a přetěžování jediného prvku sítě.

Hlavní serverovna je umístěna v srdci hlavní budovy školy. V této místnosti je v hlavním rozvaděči ukončeno cca. 300 kabelů z různých částí školy, dále je zde ukončen přívod všech optických kabelů a to jak páteřních LAN, tak i přívodu poskytovatele připojení. Do hlavního switchu jsou přivedeny páteřní linky vedoucí ke koncovým switchům. Teprve do těchto switchů jsou připojovány koncové počítače, tiskárny, a jiná zařízení (např. jednotky přístupového systému, jednotky systému pro výdej stravy, kamery, WiFi AP, apod.). Switche jsou do páteřního L3 switchu připojeny buď přímo metalicky, popř. přes optické trasy pomocí převodníků (buď externí krabičky nebo SFP moduly). Podružné rozvaděče jsou dále v nejvyšším patře hlavní budovy (8 vláken SM 9/125 + 2 × cat. 6 + 2 × cat. 5e), v přístavbě tělocvičny (zde jsou kabinety, dílny, jedna třída, kamery, telefony, wifi, atp.; 8 vláken SM 9/125 + 2 × cat. 6) a pak po jednom na přilehlých budovách dílen odborného výcviku. (2 × 4 vlákna MM 62,5/125). Počet vláken a metalických kabelů převyšuje potřebu s ohledem na rezervy pro budování dalších sítí. Z aktuálních plánů školy lze uvést např. přímé propojení switchu v každé PC učebně dvěma kabely do páteřního L3 switchu za účelem zkrácení cest a latencí a maximalizace spolehlivosti. Každý switch má pro přenos dat mezi klienty a hlavním switchem k dispozici dvě nezávislé trasy, jejich využití v závislosti na podmínkách řídí protokol LACP. Tento protokol umožňuje správci v případě potřeby přepojovat páteřní linky bez výpadku konektivity. Každá páteřní linka má rychlost 1 Gbps, přístupové porty pak 100 Mbps.

Síť využívá celkem 27 virtuálních segmentů sítě (VLAN) odpovídajících IP podsítím (L3 subnet). Tyto segmenty jsou vytvořeny pro jednotlivé servery, dále pro jednotlivé třídy koncových bodů (např. počítače v kabinetech, ve třídách, na ekonomickém úseku, v pracovních vedení, veřejný rozsah pro osobní zařízení žáků a zaměstnanců bez dohledových nástrojů, každá PC učebna má vlastní podsíť, ...) a pak se jedná právě o bezpečnostní systémy jako kamery, přístupový systém, EZS (alarm) přes LAN nebo sekundární server na jiné fyzické lokalitě pro zálohování dat.

Řízení adresace v síti má na starost DHCP server na virtuálním stroji, který zároveň slouží jako doménový řadič platformy Active Directory. Tento server slouží také pro běh DNS, WINS a tiskových služeb. Služba DNS uvnitř sítě funguje diferencovaně pro jednotlivé podsítě. Zatím co pro některé podsítě, primárně ty veřejné, jsou využity pouze externí DNS servery, pro interně důležité podsítě (počítače vedení, kabinety, ekonomický úsek, ...) jsou zdefinovány servery na interní DNS. V interní DNS zóně jsou totiž oproti veřejné zóně k dispozici další subdomény sloužící primárně pro urychlení práce s interními službami, jako je např. monitoring. Škola využívá systém blokování nevhodného obsahu dle blokování webů v závislosti na jejich

kategorizaci, a to na úrovni DNS. Jiné než povolené DNS servery jsou v síti blokovány. Mezi blokované položky patří např. weby s tematikou pornografie, zbraní, drog, P2P trackery, známé stránky obsahující malware, spyware nebo adware, známé podvodné a phishingové stránky, blokace systémů k obejití ochran + anonymizéry, spamové domény, gambling, hacking, keyloggery, tematika podvodů, nechutnosti, a další podobné kategorie.

Škola využívá služeb VPN a to jednak pro zaměstnance (administrátoři a účetní), pro něž je nasazeno L2TP / IPsec s šifrováním 3DES pomocí předsdíleného klíče (preshared key), jednak ale využívá VPN i pro již zmíněné spojení sítí hlavní budovy a internátu, kde je nasazen OpenVPN spoj s šifrováním AES256. Obě šifry jsou považovány za bezpečné.

Jak již bylo zmíněno, SŠ disponuje vlastním serverem, v současnosti 5 let starým, na němž je díky virtualizaci provozováno 10 virtuálních serverů. Mezi ně patří např. server pro vnější služby (několik webů včetně webové aplikace Bakaláři, databáze pro weby, PHP, FTP), pro učitele (databáze ŠVP, souborové služby, Bakaláři), pro vedení (účetní systémy, souborové služby), pro výuku (výukový software, souborové služby), provozní server pro správu přístupového systému, server síťové infrastruktury (AD, DHCP, DNS, WDS, WINS, tiskové služby, ...), server monitoringu Zabbix, server WSUS a knihovní a meteo systém. Server je modelově i technicky shodný se serverem používaným studovanou základní školou s malým rozdílem. Pro účely SŠ přestal s rozvojem technologických celků dostačovat výkon úložiště a velikost operační paměti, byly proto zakoupeny dva SSD disky Samsung 850 Pro o velikosti 512 GB a kit DDR3 1600 MHz ECC o kapacitě 32 GB (4 × 8 GB). Původní SAS disky byly ponechány funkční, avšak pouze jako stabilní velkokapacitní úložiště dat a pro účely provozních záloh, nikoliv na provoz operačních systémů. Nové SSD byly spojeny do RAID 1 softwarově a to z důvodu eliminace problémů s vyčítáním SMART dat před existující SAS řadič. Navíc tento řadič nepodporuje TRIM. Na serverech probíhá denně zálohování důležitých denních dat, jako jsou databáze nebo soubory webů. Jednou týdně pak probíhá zálohování celých serverů a to na zvláště vyčleněný záložní server, který je umístěn ve stavebně oddělených prostorách na druhé straně školy. Tento server má rovněž disky v softwarově řešeném RAID 1. Softwarová údržba serveru probíhá cca. jednou měsíčně, hardwarová jednou ročně.

Nejstarší síťový prvek v síti je nyní starý 3 roky, nejmladší necelý rok. Síť byla průběžně inovována s probíhajícími etapami celkové rekonstrukce elektroinstalace, přičemž došlo ke sjednocení využívané technologie, vyřazení parametricky a výkonově nevyhovujících zařízení a zavedení monitoringu síťových prvků. Vzhledem k proběhlé unifikaci síťového prostředí má škola na skladě jeden rezervní switch a router každého typu (včetně napáječe) pro případ náhlého



selhání. Všechny konfigurace síťových prvků jsou uloženy lokálně u administrátorů a také v cloudovém úložišti. Nastalou situaci tak lze v době přítomnosti jednoho ze správců do půl hodiny vyřešit.

Veškeré provozní parametry, včetně hlášení o stavu úložišť, zaznamenává s využitím upravené šablony monitorovací systém Zabbix. Chybová hlášení tohoto systému jsou reportována na e-mail administrátora.

Správce má rovněž sepsány metodiky pro kontroly bezpečnosti a spolehlivosti, které průběžně vylepšuje a upravuje dle získaných informací a zkušeností. Bezpečnostní audit sítě je prováděn vždy o letních prázdninách v rámci větší údržby. Zahrnuje např. kontrolu konfigurace síťových prvků, extenzivní údržbu software na serveru, prověření sdílených položek, hromadné kontroly na přítomnost malware, oslovení zaměstnanců za účelem vyžádání si hlášení i zdánlivě malicherných problémů, prověření funkčnosti systémů zálohování, prověření logů serverových služeb, extenzivní kontrola dlouhodobých záznamů monitorovacích systémů se zaměřením na provozní anomálie a kontrola fyzického stavu spravovaného majetku.

Správce má svůj e-mail zaveden do informačních systémů výrobců síťových prvků, takže při vydání důležité bezpečnostní aktualizace je neprodleně informován e-mailem. Preventivní kontroly aktualizací provádí cca. jednou za tři měsíce.

Na dotaz, zda by škola využila služeb externích bezpečnostních auditorů pro identifikaci problémů, které nemusí být na první pohled zjevné a které jsou potenciálními rizikovými místy pro útok na školu zněla odpověď vedení, že ano, ale v rámci zachování dobrých vztahů až v momentě, kdy by měli důvodné podezření na narušení bezpečnosti nebo na vyžádání správců.

Na otázku, zda má škola nastaveny kontrolní mechanismy pro ověření výsledků práce lidí zodpovědných za stav ICT padla jasná odpověď, a to, že na poradách sledují odezvu kolegů v organizaci a že vzhledem k aktivnímu přístupu správců nemají důvod svůj přístup měnit.

#### ***IV. Bezdrátové sítě***

Školám byly položeny otázky týkající se využívání bezdrátových sítí. Obě školy se shodly na názoru, že je nutné v určitém rozsahu omezit dostupnost nebo funkcionalitu těchto sítí. Obě školy mají signálem WiFi pokrytou celou plochu školy.

- ZŠ využívá školní wifi pouze k připojení počítačů, kde není vybudována strukturovaná kabeláž. SŠ využívá wifi v extenzivním měřítku pro umožnění přístupu k informacím všem návštěvníkům školy.
- Pouze SŠ poskytuje přístup k bezdrátové síti svým žákům, a to bezúplatně, bez garance funkčnosti a bez uživatelské podpory.
- Vedení i oslovení pedagogové ZŠ zastávají názor (s nímž autor nemůže jinak, než souhlasit) a to, že jednou z hlavních úloh základní školy je vystavit žáky v maximální možné míře vzájemné sociální interakci a že technologie ji omezující by na vývoj žáků měly mít v tomto vývojovém období, zvláště v prostředí školy, minimální vliv.
- Zástupci obou škol se shodli na tvrzení, že je nutné naučit žáky tyto technologie využívat pro účely jiné, než je vlastní zábava.
- ZŠ využívá více vzájemně nekomunikujících levných komerčních routerů, jelikož od sítě nevyžaduje vysoký výkon a jelikož byl při realizaci sítě kladen důraz na cenu. SŠ využívá enterprise-class zařízení od firmy Aruba Networks (dnes HP), což je řešení centralizované a sloučené pod jednotnou správu prostřednictvím kontroléru. Ten je však pro úsporu nákladů pouze virtuální a jeho roli přebírají jednotlivé přístupové body podle režimu multi-master – pokud dojde k výpadku komunikace s kontrolérem, algoritmus na základě složitých kritérií vybere, které AP tuto roli převezme. AP v roli kontroléru i nadále poskytuje standardní služby bezdrátovým klientům.
- SŠ využívá vysílání dvou sítí (SSID) z každého AP – učitelské a žakovské.
- Učitelská síť je na obou školách chráněna šifrováním WPA2 a předsdíleného klíče. V případě obou škol kombinuje heslo malá a velká písmena a číslice. ZŠ využívá nestandardní heslo o jedenácti symbolech obsahující slova, SŠ využívá náhodně generované heslo o čtyřiceti nezaměnitelných znacích (pro omezení omylů při zadávání). SŠ plánuje po kompletní integraci elektronických systémů přechod na jednotné uživatelské identity a ověřování prostřednictvím 802.1x.
- V obou školách je přístupové heslo známo pouze administrátorovi, ten jej zadá do školou vlastněných a spravovaných zařízení na vyžádání, popř. při instalaci. V mobilních zařízeních spravovaných SŠ (Android, iOS) jsou tato hesla navíc instalována se spravovanou jednotnou konfigurací prostřednictvím mobilního managementu

(Google MDM). Uživatelé stačí přihlásit se do svého školního účtu. Tato služba je školám poskytována v rámci GSuite for Education zdarma.

- Žákovská síť na SŠ je provozována bez šifrování a omezení přístupu. Vedení školy zastává názor, že naplňuje právo na svobodný přístup k informacím s bezpečnostními omezeními vedoucími k ochraně rozvoje osobností svých žáků (viz následující bod).
- ZŠ na celé síti, včetně bezdrátové, nevyužívá filtrování nevhodného obsahu. Žáci nemají k počítačům přístup. SŠ využívá filtrování obsahu ve dvou stupních. První je již popsáný, benevolentní content filter na úrovni centrální DNS pro odfiltrování vysloveně nebezpečných a nevhodných stránek, druhý je L7 filtr na úrovni firewallu na přístupových bodech pro wifi. Na učitelské síti je filtrován opět pouze nebezpečný obsah (viry, malware, porno, atp.), na žákovské síti je pak filtr nastaven mnohem přísněji. Stránky jsou jednak filtrovány dle ratingu bezpečnosti, kdy stránky hodnocené jako vysoce rizikové jsou blokovány, kategorizační filtr pak blokuje kromě standardních výše popsáných kategorií primárně peer-to-peer síť a kvůli kyberšikany i sociální síť. To je však s ohledem na šifrovaný provoz poněkud problematické, dochází tak ke spolehlivému blokování webových rozhraní, ale pouze většiny funkcí mobilních aplikací. Základní funkcionalita, tj. textová komunikace, většinou zůstává s ohledem na dynamický charakter těchto služeb funkční. L7 firewall na přístupových bodech je založen na cloudovém řešení Brightcloud, který využívá kromě standardního blacklistingu, kategorizace a klasifikace webů i hlubší analýzu provozu za účelem detekování specifického chování aplikací, je tak mnohem flexibilnější a méně jednoduše obejitelný. Pravidla pro blokování definuje správce sítě ve spolupráci s výchovným poradcem a preventistou sociopatogenních jevů. Schvaluje zástupce ředitele.
- ZŠ firmware používaných wifi routerů neaktualizuje, jelikož jsou již zastaralé a firmware pro ně není dále vyvíjen. SŠ aktualizuje firmware systému v závislosti na seznamu změn obsažených ve vydaných aktualizacích s ohledem na bezpečnost a co nejmenší zásahy do sítě pro zachování funkčnosti.
- V bezdrátové síti ZŠ jsou zastoupeni 4 různí výrobci, v síti SŠ jediný a dokonce i jediný model AP.
- SŠ využívá pro správu AP dva oddělené systémy, jeden pro školní kampus a druhý výhradně pro internát. Toto rozložení má za cíl omezit poruchy při výpadku spojení mezi

budovami a rozdělit možnosti konfigurace těchto systémů s ohledem na jiné podmínky v obou lokalitách.

- ZŠ si je vědoma rizika vyplývajícího z využívání funkcí WPS (wireless protected setup) a UPnP, proto je má na využívaných zařízeních vypnutý. Pro systém SŠ toto není aplikovatelné, jelikož se jedná o enterprise-class systém.

## **V. Datové služby**

Každá organizace využívá různých datových aplikačních služeb, jejichž vhodné využití může organizaci přinést výhody i problémy v případě nezajištění dostatečné bezpečnosti využívaných dat. Následující řádky zkoumají logickou (nikoliv fyzickou) bezpečnost dat v organizacích.

- Obě oslovené školy využívají vlastních zdrojů k hostingu webových služeb.
- Oslovené školy hostují dvě shodné webové služby – školní web a webové rozhraní systému Bakaláři. SŠ navíc využívá i další webové systémy, např. e-learning Moodle, proprietární systém pro rezervace pronajímaných prostor, projektové weby (EU) nebo pouze interní webové služby jako je monitoring (Zabbix) nebo správa databází prostřednictvím webového rozhraní (PHPmyAdmin).
- Ani jedna z oslovených škol nevyužívá na školním webu pro přenos dat mezi klientským zařízením a školním serverem šifrování komunikace (SSL / TLS).
- ZŠ nevyužívá šifrování ani pro přenos dat webového rozhraní systému Bakaláři. SŠ využívá šifrování TLS 1.2 se zpětnou kompatibilitou na TLS 1.1 a důvěryhodného certifikátu podepsaného certifikační autoritou Comodo, avšak pouze pro systém Bakaláři a to kvůli ochraně osobních údajů a citlivosti zpřístupňovaných dat.
- Obě školy mohou měnit obsah školních webových stránek přímo v rámci školy, SŠ má navíc díky redakčnímu systému více redaktorů webu s propracovaným systémem zodpovědnosti a přístupových práv.
- Obě školy mohou přímo zasahovat do struktury webových stránek, nemají žádná autorská ani technická omezení, záleží jen na nastavených vnitřních procesech organizace. Na ZŠ se o web školy stará přímo správce sítě, který je zároveň tvůrcem i editorem webu

a dobře zná jeho kód. Na SŠ fungují strukturální změny v rámci zaslání požadavku na externího tvůrce webových stránek (úkolový zaměstnanec živnostníka), který je následně v dohodnutém termínu upraví. Tyto změny jsou ale spíše výjimkou. O aktualizace a zálohování webu se na SŠ stará správce sítě, o obsah zodpovědný zaměstnanec školy.

- Weby jsou na obou školách denně zálohovány.
- Ve využití cloudových služeb se obě zkoumané školy liší. ZŠ nevyužívá žádné e-mailové služby si hostuje na vlastním serveru. SŠ je naopak využívá velmi extenzivně.
- SŠ využívá platformu GSuite for Education (v rámci projektu podpory rozvoje škol společností Google jsou tyto služby poskytovány školám zcela zdarma), z níž využívá mnoho služeb. Jako hlavní uvádí službu e-mail s kvalitním filtrováním spamu na bázi algoritmů používaných pro Gmail a vysokou dostupností, a Google Disk (Drive) s možností využít neomezené cloudové úložiště. Výhodou cloudové platformy je, že se o její bezpečnost a provoz stará externí subjekt s finančními a technologickými možnostmi výrazně přesahujícími možnosti školy čili i dostupnost systémů a např. možnosti práce na mobilních zařízeních nebo integrovanost s dalšími službami jsou nesrovnatelné s provozem vlastních systémů, o pořizovacích a provozních nákladech srovnatelného datového úložiště ani nemluvě. Veškerý provoz mezi cloudovými servery a koncovým zařízením pracovníka je šifrovaný, rovněž data jsou na serverech Googlu ukládána šifrovaně a je dobře zdokumentován proces s jejich nakládáním. Škola v testovacím režimu zkoušela i cloudové řešení Office 365 a rozhodla se pro upuštění od tohoto scénáře z důvodu přílišné komplikovanosti systému, zahlcování správců reklamou a malých konfiguračních možností ve srovnání s platformou GSuite.
- Ani jedna z oslovených škol nemá ve svých budovách instalovány infokiosky a ani jedna škola jejich zavedení nevidí jako prioritu, ale nevyklučuje jej.
- Ani jedna z oslovených škol nemá ve svých budovách instalovány veřejné informační obrazovky. Do budoucna je zvažuje pouze SŠ.
- Pouze SŠ poskytuje svým žákům xerografické služby a to veřejnou kopírku formátu A3. Kopírka je veřejně přístupná na chodbě a funguje na bázi čipových karet. Do budoucna je plánována v rámci projektu integrace její výměna za nové zařízení umožňující práci s RFID kartami standardu Mifare pro možnost využití jednotných školních karet

shodného formátu s kartami ISIC. ZŠ o zavedení těchto služeb neuvažuje, jelikož pro ně nemá využití.

- Ani jedna škola v současnosti nevyužívá systém pro řízení tiskových služeb. O jeho zavedení delší čas usiluje SŠ, pro školu to však znamená napřed vyměnit nevyhovující lokální tiskárny za síťové, zavést jednotný systém uživatelských identit a investovat do pořízení tohoto řešení. ZŠ tisk pedagogů neomezuje, funguje zde však dohoda, že tisk je používán v co nejmenší míře a pedagogové pro rozmnožování potřebných pracovních listů použijí ekonomickou A3 kopírku.

## **VI. Počítače**

- Na ZŠ se nachází přibližně 50 počítačů, na SŠ přibližně 230. ZŠ nemá v majetku ani jeden notebook, SŠ jich má 84 a snaží se je postupně vyřadit. Tyto hodnoty vycházejí z dat poslední inventarizace a v průběhu roku se mění s průběžnými nákupy a vyřazováním.
- SŠ využívá notebooky např. do laboratoří jako mobilní měřicí pracoviště, k výuce v rámci odborného výcviku, k pracovní mobilitě pedagogů a vedoucích zaměstnanců a místy i jako stabilní PC tam, kde není k dispozici dostatek místa. Jelikož však mají notebooky oproti stabilně instalovaným PC nízkou životnost, vysokou poruchovost a pořizovací cenu, škola se jejich využití snaží eliminovat pouze na nejnnutnější případy.
- SŠ disponuje třemi učebnami, průměrně pro 17 žáků. V současné době je připravován projekt na realizaci nové učebny pro 34 žáků. ZŠ disponuje jedinou PC učebnou, k dispozici je 16 lepších PC, v případě potřeby je možno využít i starších počítačů a pracovat tak s celou třídou.
- ZŠ nakupuje výhradně novou výpočetní techniku prostřednictvím malého živnostníka, který je škole údajně ochoten nastavit rozumné ceny. SŠ se vydala cestou nákupu repasovaných počítačů a to primárně vzhledem k omezenému rozpočtu, v současnosti nízkým nárokům na výpočetní výkon a cenovému rozdílu oproti novým strojům. Cenový limit na počítač si stanovili na 6000,- Kč s DPH a minimální požadavky jsou 120GB SSD, 4 GB DDR2 na frekvenci 800 MHz, dvoujádrový procesor střední výkonové třídy min. z roku 2010, kvalitní zpracování šasi a min. po jednom grafickém výstupu analogovém a digitálním (levné redukce jako např. DVI-I → D-Sub připouští). Vzhledem

k ceně PC je jejich případná investice do oprav nevýhodná, škola vždy nakoupí o pár ks více do zásoby.

- Počítače ve třídách jsou nejsou ani v jedné škole fyzicky chráněny před odcizením. Jednak je toto složitě realizovatelné s ohledem na zajištění provozního chlazení zařízení, dále v případě ZŠ jsou třídy pod prakticky neustálým dohledem pedagogů a v případě SŠ by investice do nábytku byly vyšší, než případné škody.
- Po stránce logiky jsou v obou školách počítače chráněny správcovským heslem, uživatelé mají omezená uživatelská práva za účelem minimalizace rizik spojených s malwarem nebo nezáměrným, ale i cíleným poškozováním software a systémové konfigurace. Všechny počítače v obou školách mají rovněž heslem chráněný přístup do rozhraní pro konfiguraci BIOS / UEFI.
- Správci na obou školách mají definovaný softwarový standard pro instalaci klientských stanic. Správce ZŠ tento standard udržuje manuálně tak, že jednou ročně obejde počítače v síti s flash diskem a aktualizuje software. Správce na SŠ udržuje software aktuální prostřednictvím hromadného deploymentu aktualizací balíčků skrze centrálně definované politiky instalace, pročež využívá systém PDQDeploy.
- Zatím co správce na ZŠ instaluje každý počítač manuálně zvlášť, správci na SŠ si vzhledem k objemu práce tuto práci usnadnili vytvořením jednotného instalačního obrazu systému a jeho automatizovaným nasazením prostřednictvím síťové služby WDS (Windows Deployment Services). Tento obraz se jednou ročně před velkým letním prázdninovým servisem aktualizuje.
- Obě školy kladně reagovaly na otázku, zda mají ve své softwarové politice zakořeněnu podporu volně dostupného software, tj. primárně open source, sekundárně freeware. Z tohoto zjištění plyne, že se školy snaží uvažovat nad faktem, zda je reálně nutné investovat do komerčního softwaru, jehož alternativy mohou využívat i zdarma. Obě školy se shodly, že i přes veškerou snahu nahrazovat volně šiřitelným softwarem komerční produkty stále existují programy, které jsou pro tyto organizace nenahraditelné. Jmenovitě shodně uvedly nutnost investic do licencí operačních systémů MS Windows (v edici Pro kvůli možnosti zařazení do školní domény Active Directory) a MS Office. Ač se otevřené kancelářské balíky OpenOffice a nověji i LibreOffice hodně změnily k lepšímu, v komerčním MS Office jsou stále funkce, které jimi plně nahradit nelze, popř.

jen velmi složitě. Na otázku kolik procent softwaru využívaného v organizaci představuje v součtu freeware a open source odpověděly školy následovně:

- ZŠ: přibližně 80 %
- SŠ: přibližně 90 %

Tyto hodnoty lze vysvětlit zvýšeným podílem komerčního vzdělávacího softwaru zaměřeného na seznámení žáků s adekvátně didakticky transformovaným obsahem na základní škole. Na škole střední se vyučují již spíše praktické dovednosti pro práci s běžně dostupným softwarem a není zde výrazná potřeba utrácet za komerční software. Zatím co ZŠ uvedla, že komerční software využívá pro výuku oborově specifických témat (např. matematika, čeština, angličtina, atp.), SŠ uvedla, že je pro ni prioritní komerční software pro psaní všemi deseti (Mount Blue), účetní systém Pohoda a proprietární software pro odborný výcvik (s ohledem na zachování anonymity školy autor neuvádí konkrétní data, jedná se o software pro diagnostiku zařízení a plánování specifické produkce a údržby).

- Školy dodaly následující údaje o průměrných ročních investicích za posledních 5 let:
  - Základní škola:
    - Software: 20.000,- Kč (= 0,8 % ročního provozního rozpočtu)
    - Hardware: 70.000,- Kč (= 2,8 % ročního provozního rozpočtu)
    - Celkem základní škola utrácí za ICT 3,6 % ročního provozního rozpočtu.
  - Střední škola:
    - Software: 55.000,- Kč (= 0,64 % ročního provozního rozpočtu)
    - Hardware: 240.000,- Kč (= 2,79 % ročního provozního rozpočtu)
    - Celkem střední škola utrácí za ICT 3,43 % ročního provozního rozpočtu.
- ZŠ nespolupracuje s externími subjekty za účelem využití jimi vyřazovaného ICT materiálu, vystačí si s vlastními zdroji, což svědčí o stabilním ICT politice. SŠ naopak v minulosti realizovala dva projekty přejímky vyřazovaných počítačů, poprvé ze Státního zastupitelství, podruhé z velké výrobní firmy podnikající v oblasti automotive, která vyřazuje stále využitelnou výpočetní techniku plánovaně s koncem její morální životnosti a nahrazuje ji technikou výkonnější, což je např. v případě pracovníků pracujících v oblasti fyzikální simulace velice podstatný faktor. Pomocí těchto realizovaných



projektů zkoumaná SŠ úspěšně dohnala předchozí správou zanedbávané investice do ICT.

## **VII. Telefonie**

Obě studované školy jsou vybaveny telefonními přístroji. Zde je však možné pozorovat obrovské rozdíly, jelikož v těchto organizacích funguje jiný provozní systém. Zatím co na studované ZŠ jsou všichni pedagogové koncentrováni do jediné sborovny, na studované SŠ mají vždy vlastní kabinet. Ty mohou být navíc různě rozprostřeny do celého areálu školy. Na ZŠ tak odpadá značný problém v podobě shánění svých kolegů v případě potřeby. Rovněž v případě, že se pedagoga snaží sehnat rodiče, je tento úkol snazší na ZŠ, než na SŠ – pokud totiž zrovna daný člověk odešel cokoliv řešit, je na SŠ pro rodiče prakticky nedosažitelný a jediné co člověku zbývá je zavolat na sekretariát a poprosit o předání zprávy či kontaktu, což se nakonec stejně většinou stane e-mailem. Na ZŠ mohou danému člověku zprávu předat přímo kolegové. Díky tomu je pak možné vysvětlit markantní rozdíl mezi třemi pevnými linkami existujícími na studované ZŠ a třiceti sedmi linkami v případě SŠ.

- ZŠ využívá tři výhradně analogových linek vyvedených přímo do veřejné telefonní sítě a připojených na tři standardní drátové analogové telefony.
- SŠ využívá interní hybridní pobočkovou telefonní ústřednu Panasonic KX-TDA100. Z této ústředny je do hlavního rozvaděče vyvedeno celkem 48 portů, z toho 8 digitálních (nejedná se o VoIP v pravém slova smyslu, jde o proprietární digitální protokol společnosti Panasonic, která si tímto krokem pojistila kus trhu). Ne všechny jsou obsazeny, aktivně je využíváno celkem 37 linek. Celkem je využito 6 digitálních telefonů a 31 analogových, z nichž je 8 přístrojů bezdrátových (standard DECT využívající jednu základnu na jeden telefon).
- V budově SŠ mohou uživatelé využívat systém vnitřních klapek (100-148). V ZŠ bylo autorovi řečeno, že tento systém možná mají také, ale že mají rychlejší vstát ze židle a dojít do vedlejší místnosti. Místní telefonní síť zde nemá význam.
- SŠ v současnosti chystá přechod z poruchové hybridní ústředny na systém VoIP. V rámci tohoto projektu škola analyzuje vhodnost zavedení buňkového DECT systému Well RTX za účelem zlepšení dosažitelnosti pracovníků a jejich mobility v rámci organizace. Vzhledem k nákladnosti se však škola kloní spíše k variantě realizace páteří VoIP

infrastruktury, otestování nové funkcionality v praxi s ponecháním si možnosti rozšíření systému v budoucnosti o bezdrátovou část. Odhad ceny realizace VoIP v celé škole byl stanoven na 250 tis. korun, což představuje investici ve výši necelých 3 % ročního rozpočtu na provoz školy. Jedná se tak o praktické vyčerpání ročního rozpočtu na hardware, návratnost investice však byla spočítána na necelé tři roky.

- Obě školy mají uzavřeny rámcové smlouvy na telekomunikační služby prostřednictvím svých zřizovatelů. Tyto smlouvy se vztahují na pevné i mobilní služby. ZŠ vzhledem k nízkému počtu zaměstnanců a z toho vyplývající nízké administrativní zátěži svým pracovníkům nabízí možnost připojení svých telefonních čísel pod rámcovou smlouvu školy, což jim zároveň umožní volání zdarma v rámci virtuální sítě zahrnující všechna mobilní čísla po smlouvou školy. SŠ má tuto možnost také, ale administrativní zátěž při čtyřnásobném počtu zaměstnanců (a několikanásobném počtu v případě umožnění přístupu i jejich rodin) by byla neúnosná. Z tohoto důvodu škola omezila mobilní smlouvy pouze na nejdůležitější pracovníky s nutnou mobilitou a vedení organizace.
- Obě školy mají v současnosti extra dodavatele servisních služeb telefonních přístrojů. Na ZŠ proto, že telefony jsou připojeny přímo do veřejné sítě, servisní služby tedy poskytuje přímo telekomunikační operátor. Na SŠ je to primárně z dnes již historického důvodu, kdy proto, aby člověk mohl spravovat danou analogovou nebo hybridní telefonní ústřednu, musel podstoupit zvláštní certifikační školení u autorizovaného školitele. Výrobci si navíc pojišťovali závislost klientů na těchto certifikovaných technicích i tím, že pro správu ústředny potřeboval člověk buď speciální hardware, speciální software nebo (z pohledu výrobce) nejlépe obojí. Moderní VoIP ústředny tyto problémy do značné míry odbourávají využíváním otevřených a standardních komunikačních protokolů, připojení do standardní ethernetové sítě a přístupností konfiguračního rozhraní ústředny přes standardní webové rozhraní. To do značné míry otevírá dveře zájemcům o naučení se principů dané ústředny, k čemuž výrobci většinou poskytují bohatou dokumentaci. Toho chce škola využít a s plánovaným přechodem na VoIP chce tuto zodpovědnost přenést na vlastní správce sítě.

## VIII. Elektronické zabezpečovací systémy

- EZS jsou aktivně využity v obou dotázaných školách. Na ZŠ je využíván jen základní drátový systém s napojením na pult centrální ochrany, na SŠ jsou systémy dokonce dva.
- ZŠ využívá EZS k ochraně společných prostor (chodeb), přístupových dveří do objektu a kanceláře školy, kde je zároveň instalována ústředna EZS. Aby se mohl člověk dostat ke školnímu serveru, je nutné, aby prošel celou budovu do nejvyššího patra. Po cestě se nachází několik PIR detektorů. Využity jsou zde detektory magnetické na ochranu vchodových dveří a pohybové chodbové PIR detektory pro detekci pohybu ve společných chodbách.
- SŠ využívá jeden systém k hlídání hlavní budovy, konkrétně počítačových učeben a kanceláře zástupce ředitele školy, kde je umístěna ústředna EZS. Tento systém kombinuje detektory bezdrátové v učebnách a v místnosti s ústřednou je využit detektor sběrnicový. Ovládací klávesnice systému je umístěna v témže kabinetu. Druhý systém, tentokrát výhradně bezdrátový, slouží k hlídání objektů odborného výcviku, kde slouží k hlídání dílen, skladů materiálu a kancelářských prostor. Společné chodby nejsou pokryty z organizačních důvodů.
- Obě školy využívají služby společností zajišťujících chod vlastního pultu centrální ochrany, na které jsou systémy napojeny. Tyto společnosti školám rovněž zajišťují servis zabezpečovacích systémů.
- Ani jedna z oslovených škol nevyužívá potenciál ústředny EZS pro účely automatizace. Stejně tak oslovené školy nevyužívají ani vzdáleného ovládání přes dedikovaná zařízení komunikující prostřednictvím mobilní sítě.
- Ani jedna z oslovených škol nevyužívá v kombinaci s EZS environmentální detektory. Jak ZŠ, tak i SŠ však mají detektory zemního plynu a oxidu uhelnatého nainstalovány v kotelně školy, kde slouží pro případné odstavení topných systémů.

**Komentář:** Na ZŠ je systém postačující a slouží svému účelu dobře. Jako vhodné se jeví rozšířit systém na hlavní budově SŠ o hlídání pohybu v serverovně, vlastní klávesnicí pro serverovnu a o požární detektor v téže místnosti. Stejně opatření se jeví jako vhodné v místnosti se záložním serverem a digitalizačním terminálem maturit. Požární detektory by bylo rovněž vhodné rozmístit

ve školní knihovně, archivu, sborovně a na ekonomickém úseku, kde je velké množství uskladněného papíru, dále v chemickém skladu a všech dílnách, kde se vyskytuje množství hořlavin a okysličovadel (v dílnách také potenciálních zdrojů tepla) a také v aule, kde se nachází množství kontinuálně napájené elektroniky.

## **IX. Elektronické vstupní systémy**

- Ze zkoumaných škol využívá EVS pouze střední škola.
- Základní škola uvedla, že je pro ni tento systém zbytečný hned z několika důvodů. Vstup do školy je řízen jejími zaměstnanci a to buď prostřednictvím zvonku nebo dozorujícího pedagoga, jenž má v danou chvíli dozor u hlavního vchodu. Zadní vchody do budovy bývají běžně zvenčí nepřístupné. Vedení školy ale uvedlo případ, kdy jeden ze zaměstnanců zapomněl po pronesení nákladu vchod zavřít a jelikož byla zrovna otevřená brána do dvora, kolemjdoucí zloděj pravděpodobně vycítil příležitost a ve škole vykradl otevřenou sborovnu. Podobným situacím, kdy si zaměstnanec cíleně zablokuje dveře, však EVS zabránit ani nemůže. Poslední zmíněným důvodem pak byl obrazný popis situace, kdy by žákům na prvním stupni měli rozdat přístupové čipy...
- SŠ využívá přístupový systém na celkem pěti vchodech v hlavním komplexu a jediném vchodu na školní internát. Každý žák a zaměstnanec je vybaven přístupovou kartou nebo čipem, přičemž identifikace je zajištěna čipy Mifare. Primárními identifikačními médii tak jsou v případě žáků průkazy ISIC, v případě učitelů případně ITIC, každý žák či zaměstnanec má také právo vypůjčit si za vratnou kauci 200,- Kč školou vydanou kartu nebo čip ve tvaru přívěšku na klíče. Systém spravuje správce sítě na žádost vedení v případě zaměstnanců a na žádost třídních učitelů v případě žáků. Žáci a zaměstnanci jsou přiřazeni do odpovídajících skupin v závislosti na povolených přístupových cestách a povolených časových intervalech, kdy mohou těmito cestami projít. Žáci mají přístup povolen denně od 5:30 do 19:00, učitelé stejně tak, učitelé však navíc mohou využít přístupové cesty pro návštěvy (mimo šatny). Je tak zajištěn i jejich volný pohyb mezi budovami v rámci kampusu. Zapomene-li si někdo v budově kartu, odejít přes zabezpečené dveře může jedině pomocí rozbití sklíčka a stisknutí nouzového tlačítka, jehož aktivace kromě otevření dveří také rozešle varovné e-maily, zapomenuté karty se tak řeší spíše výjimečně, když někdo projde s dalšími lidmi ven, ale dovnitř už

se nedostane. Dveře jsou blokovány magnety o síle několika kN, jejichž napájení je zajištěno zálohovaným zdrojem u každých dveří. V případě výpadku energie tato jednotka dokáže zajistit napájení na 2 hodiny nepřetržitého provozu.

- Systém umožňuje prohledávání historie průchodů neomezenou dobu nazpět (v závislosti na nastavení systému), a to prostřednictvím webové aplikace běžící na vyhrazeném serveru. Na tomto serveru běží kromě webového serveru rovněž aplikační backend zajišťující komunikaci s řídicími jednotkami jednotlivých vchodů.
- Popisovaný systém má jedinou, zato obrovskou chybu – po otevření dveří se dají dveře čímkoliv zablokovat v otevřené poloze a může jimi projít prakticky kdokoliv. Z tohoto důvodu byly na škole odstraněny ze vchodových dveří zárážky. Z tohoto důvodu, stejně jako proto, že identifikaci v případě ranního davu vystoupivšího z MHD má systém jen u prvního člověka, se škola rozhodla v extenzivní míře nasadit právě níže diskutovaný kamerový systém. Ač si škola byla tohoto problému vědoma již před realizací, musela projekt realizovat tímto způsobem z ohledem na dostupné finance a „Metodické doporučení“ (což si vedení škol po předchozích zkušenostech a nejasnosti komunikace MŠMT vykládá již zásadně jako „závazné nařízení“) uvedené v příloze č. 2 této práce. Vedení školy rovněž potvrdilo domněnku autora, a to že by systém bez vzniku tohoto dokumentu na základě žďárské kauzy mezi prioritami opravdu nebyl, jelikož jde, vzhledem k možnostem útočníků a škol, nemluvě o cíleně zamýšlené veřejné přístupnosti školních pozemků s téměř stoletou tradicí, pouze o úřednický alibismus.

## **X. Kamerové systémy**

- Ani jedna z oslovených škol dosud nevyužívá kamerové systémy, obě dvě však jejich zavedení plánují.
- ZŠ by ráda nainstalovala do svého areálu čtyři kamery. Tři interiérové kamery by měly hlídat veřejně přístupnou předsíňku, kde rodiče čekají na odchod dětí ze školy, dále hlavní schodiště spojující jako jediné všechny přístupové cesty do budovy s vyššími patry a posledně hlavní vchod do školy zevnitř tak, aby byly pokryty zároveň přístupové cesty z dalších dvou zadních vchodů. Čtvrtou kameru by škola ráda nainstalovala na školní dvůr, kudy do budovy vnikl zloděj při poslední řešené krádeži. Všechny kamery by měly

mít rozlišení Full HD, EXIR přísvit v infračerveném spektru, dostatečnou citlivost pro noční snímání a taktéž by měly mít záznam na dedikovaném serveru. Součástí realizace projektu bude rovněž zbudování nových kabelových tras v chráničkách zasekaných pod omítku. Odhadovaná cena projektu činí 60 tis. korun s DPH.

- SŠ v realizovaných etapách rekonstrukce elektroinstalace připravila kabelové vývody propojené do příslušných rozvaděčů na místech, kde by se v budoucnu mohly nacházet informační televize, infokiosky a kamery. Z tohoto důvodu se nyní čeká pouze na uvolnění finančních zdrojů potřebných na nákup potřebného materiálu a realizace budování kamerového systému může začít. Škola by ráda pokryla kamerami každý vchod do budov školního kampusu ve směru příchodu i odchodu, v dalších etapách by případně ráda umístila kamery i na vybrané chodby s ohledem na možnost odcizení drahé výbavy z auly či laboratoří. Zvýšená pozornost je rovněž věnována prostorám přístupným v odpoledních hodinách nájemcům tělocvičen. Celkem je v současnosti uvažováno o přibližně třiceti kamerách se záznamem, pro který bude nutno vybudovat dedikovaný výkonný server s velkým datovým úložištěm. Odhadovaná cena projektu je 350 tis. korun včetně DPH.

## ***XI. Ostatní elektroinstalace***

Budova ZŠ prochází podle tvrzení vedení první větší rekonstrukcí elektroinstalace (mění se více, než vypínače a zásuvky) od osmdesátých let teprve v posledních letech a to po etapách s ohledem na nákladnost celého projektu a volné finanční zdroje. Elektrické rozvody jsou ale dle slov vedení ještě leckdy vedeny v asfaltu izolovaných kabelech, což nasvědčuje vše tomu, že kompletní rekonstrukce elektroinstalace v budově nemusela být provedena i více, než 50 let.

Podobná situace panovala do léta roku 2013 i na škole střední, kdy byla započata první etapa celkové rekonstrukce veškerých elektrických rozvodů v budově, ať silnoproudých nebo slaboproudých. K září roku 2016 byly ukončeny práce, na které bylo z rozpočtu zřizovatele vyčleněno na účelových dotacích přes 12 mil. korun.

Průběh probíhajících rekonstrukcí na obou historických školách měl / má podobný průběh. Po odpojení přívodů elektrické energie do dané části objektu se sbíječkou rozbijí zdi v okolí původních rozvodů, ty se vytrhají ze zdi, zlikviduje se vše, co se ve zdi najde a ví se jistě,

že se může odpojit a následně se do cihel vyfrézují díry pro instalační krabice, ty se přichytí sádrou, načež se do zdí uloží silové kabely a chráničky pro slaboproudé rozvody, vše se navede do krabic, zaháže omítkou, srovná a přemaluje. Celá elektrina se tak dělá na novo podle moderních norem, jelikož izolační parametry staré kabeláže bývají za tu dobu nevyhovující a existuje zde riziko požáru.

S rekonstrukcí elektroinstalace souvisí úzce výměna světelných zdrojů. V obou dotázaných školách byly v průběhu rekonstrukčních prací nainstalována výhradně svítidla zářivková, pouze SŠ zvolila pro osvětlení tělocvičen z důvodu šetření energie světla na bázi LED. Ta nahradila původní výbojky různých typů, které jen ve velké tělocvičně měly při plném provozním výkonu spotřebu přesahující 30 kW za hodinu a oslňovaly při pohledu ke stropu, což např. při volejbalu nemuselo být úplně nejpříjemnější. Po výměně technologie došlo k úsporám energie o cca. 70 %, současný příkon činí necelých 8 kW. Svítivost jednoho takového svítidla činí 21310 lumen.

Charakteristickým rysem moderních instalovaných svítidel je přítomnost stínících mřížek, které zabraňují přímému oslnění při nepřímém pohledu na svítidlo. Tyto mřížky v kombinaci s moderními zářivkovými tělesy s kvalitními odraznými plochami a elektronickými předřadníky zvýšily efektivitu a snížily spotřebu osvětlovacích technologií v prostorech školy, zvláště pak ve třídách. Při dotazu na poměr zastoupení jednotlivých světelných zdrojů odpovědělo vedení ZŠ, že ví pouze o jediné místnosti ve škole, kde jsou ještě žárovky, jinak že jsou všechna svítidla zářivková. Obě školy dále uvedly, že ve světlech na chodbách jsou rovněž zářivky, avšak nikoliv trubcové, ale kompaktní, aby se vešly pod kulový matný skleněný kryt.

Posledním systémem, který ještě nebyl diskutován, je školní rozhlas. Základní škola uvedla, že školní rozhlas vůbec nemá instalován a že rozšíření informací po škole lze velmi efektivně dosáhnout rychlou poradou s kolegy o přestávce, případně připnutím informace na nástěnku ve sborovně. Škola nevidí důvod v zavádění systému do školy podobné velikosti.

Střední škola dokončila stavbu rozhlasových rozvodů v říjnu 2016, nemá tedy v jeho využívání velkou tradici. Dalším faktorem je absence rozhlasových rozvodů v prostorách budov odborného výcviku, kde by tím pádem došlo k rozpolcení informovanosti. Rozhlas tak plní spíše funkci evakuačního rozhlasu a prostředku pro komunikaci mimořádných sdělení.

## ***XII. Zateplení a větrání***

Budova ZŠ má zateplené stropy a vzhledem k její historické povaze nelze využít zateplení zbytku budovy obložením izolačními panely. Budova má původní okna po údržbě, i tak však dochází, vzhledem k jejich nedokonalé konstrukci, k přirozené cirkulaci vzduchu v místnostech.

Střední škola je na tom v oblasti úspory energií markantně hůře – hlavní budova nedisponuje zateplením, okna jsou původní, zdobná v neoklasicistním stylu, s nestandardním tvarem a zavíracím mechanismem, nedovírají dobře, při silnějším větru strašidelně hvízdají vlivem jejich dlouholetého opotřebení (v rámech jsou prodřené mezery...) a dochází tak k výrazným ztrátám energie. Přístavba tělocvičny je navíc montovaná ocelová konstrukce v kombinaci s obrovskými skleněnými plochami (bez moderních izolačních vlastností), její zateplení by tak bylo velice problematické. Zřizovatel i navzdory termokamerou zjištěným energetickým ztrátám nezařadil rekonstrukci mezi investiční priority a škola se tak na tyto investice dlouhodobě připravuje z vlastního provozního rozpočtu. Ve školním kampusu se rovněž nachází dvě přistavěné budovy pro praktický výcvik, novější z nich je postavena v roce 2007 za využití energeticky úsporných materiálů (duté tvárnice, povrchové zateplení). Starší sloužila původně pouze jako montovaný ocelový přístřešek pro větší vozidla, později byla vystavěny obvodové zdi a pod příhradovou konstrukcí střechy byl vybudován strop překlenutím trámy a namontováním sádkartonových desek. Tato konstrukce byla překryta izolací z minerální vaty. V roce 2016 bylo dokončeno povrchové zateplení a výměna oken i této starší budovy.

Budova školního internátu SŠ je standardní cihlový dům se sedlovou střechou, má vyměněna okna za plastová, avšak zateplení, ač je rovněž v plánu, taktéž dosud nebylo realizováno a to ani na půdě, ani obložením. Tyto úniky však nepředstavují tak markantní problém jako na hlavní budově.

Větrání všech zmíněných budov je řešeno standardně skrze otevírání oken. V souvislosti s dobou výstavby je zde záhodno vysvětlit i zvyky ze stavebnictví z doby první republiky. Každá místnost v těchto školách byla původně vytápěna vlastními kamny na dřevo, které vyžadovaly kromě komínu na odvod spalin i kvalitně dimenzovaný přívod spalovacího vzduchu. Budovy byly konstrukčně navrženy tak, že se čerstvý vzduch přiváděl samostatnými ventilačními komíny, optimálně tak, aby napřed proudil přes základy budovy a ty tak zároveň vysoušel. Toto opatření jednak kvalitně zabraňovalo vzlínání vody ze základů budovy do její konstrukce, jednak existovalo v budovách, a to i v létě, přirozené proudění vzduchu. S příchodem centrálního vytápění byly tyto komíny pro nepotřebnost zaslepeny, v případě zkoumané ZŠ dokonce i částečně zasypány. To mělo za následek několik jevů. Jednak se tyto budovy potýkají



se vztlínáním vody, což pak často draze řeší sanačními přístroji, jednak může vzniknout ve vlhkých místnostech problém se zvýšenou koncentrací mykotoxinů (plísňe) v dotčených prostorech, hlavně bylo ale zabráněno přirozenému proudění vzduchu ve třídách. Z tohoto důvodu vzniká problém s ventilací popsáný v teoretické části práce. Tento problém lze řešit několika metodami. Jednak se nabízí zachování stávajícího systému doplněného o detektory koncentrace CO<sub>2</sub>, jednak nasazení rekuperační ventilace.

Ředitelé obou škol byli po vysvětlení problému zvyšujících se koncentrací CO<sub>2</sub> ve třídách otevření postupným investicím do monitorovacích zařízení pro CO<sub>2</sub>, shodli se však na tom, že systém pro ně není prioritou, ale spíše vhodným technickým doplňkem v případě hledání vhodných investic z přebytkového rozpočtu. V oblasti rekuperační ventilace kladná odezva na dotaz k možnostem realizace systému nepřevážila, jelikož by toto opatření přineslo obrovské investiční náklady a významné konstrukční zásahy do budov s rizikem poškození stávajících instalací. Jednodušší a méně problémové řešení je proto zachovat stávající systém, případně investovat do alternativních energetických zdrojů, jako např. teplovodních solárních panelů a tepelných čerpadel. V případě SŠ také padla zmínka o úvahách nad kogeneračními jednotkami vyrábějícími kromě tepla i elektřinu. Rekuperační jednotky je na základě tohoto zjištění vhodné plánovat spíše pro nové stavby a vedení vzduchotechniky tak do nich vhodně zakomponovat.

## Závěr

Cílem této diplomové práce bylo vytvořit poznatkovou bázi z oblasti problematiky zabezpečovacích technologií. Předložená práce byla rozdělena na teoretickou a aplikační část.

V teoretické části práce byly nejprve představeny nejdůležitější základové technologie pro budování vyšších systémových celků. Následně byly popsány celky zajišťující fyzické zabezpečení budov, jejich součásti a širší možnosti aplikace. Zvláštní pozornost byla věnována podrobné analýze možností využití elektronických zabezpečovacích systémů. V této oblasti byly definovány a aplikovány do praxe poznatky a vědomosti autora z certifikačních školení majoritních výrobců těchto systémů. Dále byly porovnány a oddůvodněny přednosti a nedostatky jednotlivých metod zabezpečení budov a zhodnoceny scénáře vhodného a nevhodného nasazení. V práci byly rovněž nastíněny možnosti využití nestandardních technologií za účelem zlepšení bezpečnosti a ekonomické efektivity provozu budov, zejména škol. Na závěr byly představeny technologie mající potenciál doplnit nebo nahradit technologie současné. Rovněž byly zhodnoceny vhodné cíle v oblasti vzdělávání o popsanych technologiích.

V aplikační části práce byly konfrontovány požadavky škol dvou rozdílných typů. Na těchto školách byly demonstrovány příklady využití moderních technologií k zabezpečení jejich prostor, datové komunikace i osobních dat. Tato demonstrace probíhala formou konfrontace objektivních indikátorů s cílem dosáhnout objektivně porovnatelných a subjektivní interpretací nezkraslených výsledků. Rovněž byly zkoumány postoje vedení škol a zodpovědných pracovníků ke konkrétní problematice. Laický i odborný čtenář mohli v práci nalézt poznatky přínosné pro praxi upotřebitelnou při plánování, dozorování nebo přímé účasti na realizaci staveb budov. Význam uvedených informací byl podložen výčtem a analýzou reálně vzniklých problémových situací při realizaci popsanych projektů. Informace jsou založeny na praktických zkušenostech

S ohledem na výše uvedené lze usoudit, že dílčí cíle byly, s ohledem na omezený rozsah práce, naplněny.

## Využití zdroje

1. Historie počítačů: Od elektronky po internet. Živě [online]. 2011 [cit. 2017-04-13].  
Dostupné z: <http://www.zive.cz/clanky/historie-pocitacu-od-elektronky-po-internet/sc-3-a-147343>
2. The '90s: science and technology: When the Internet first took ahold of our lives. National Geographic [online]. 2014 [cit. 2017-04-13]. Dostupné z: <http://channel.nationalgeographic.com/the-90s-the-last-great-decade/articles/the-90s-science-and-technology/>
3. Technological Advances of the 90s. Bright Hub [online]. 2012 [cit. 2017-04-13].  
Dostupné z: <http://www.brighthub.com/education/homework-tips/articles/123405.aspx>
4. A Brief History of SoCs. Semiwiki.com: The open forum for semiconductor professionals [online]. 2012 [cit. 2017-04-13]. Dostupné z: <https://www.semiwiki.com/forum/content/1586-brief-history-socs.html>
5. The why, where and what of low-power SoC design. EETimes [online]. 2004 [cit. 2017-04-13]. Dostupné z: [http://www.eetimes.com/document.asp?doc\\_id=1276973](http://www.eetimes.com/document.asp?doc_id=1276973)
6. ZOUNEK, Jiří a Klára ŠEĎOVÁ. Učitelé a technologie: mezi tradičním a moderním pojetím. 1. vyd. Brno: Paido, 2009, 172 s. ISBN 978-80-7315-187-4.
7. Strukturovaný kabelážní systém - příručka [online]. 2017, 48 s. [cit. 2017-04-06].  
Dostupné z: [https://www.variant.cz/soubory-ve-skladu/Karty/Spol\\_Zarazene/01-MANU%C3%81LY%20CS/SKS%20prirucka%20-%20man-a4.pdf](https://www.variant.cz/soubory-ve-skladu/Karty/Spol_Zarazene/01-MANU%C3%81LY%20CS/SKS%20prirucka%20-%20man-a4.pdf)
8. Internet ve školách: jak skončil byznys za 884 milionů korun. ITbiz.cz [online]. Štěpán Beneš, 2007 [cit. 2017-04-06]. Dostupné z: <http://www.itbiz.cz/internet-ve-skolach>
9. VLČKOVÁ, Gabriela. Internet do škol - analýza efektivnosti veřejného projektu. Brno, 2006. Masarykova Univerzita v Brně. Vedoucí práce Mgr. Jiří Špalek, Ph.D.
10. SIPVZ: Proč vlastně NKÚ podává trestní oznámení? EArchiv.cz [online]. Jiří Peterka, 2002 [cit. 2017-04-06]. Dostupné z: <http://www.earchiv.cz/b03/b0814002.php3>
11. INDOŠ story. Učitelské noviny [online]. 2003 [cit. 2017-04-13]. Dostupné z: <http://www.ucitelskenoviny.cz/?archiv&clanek=3752>

12. KÁLLAY, Fedor a Peter PENIAK. Počítačové sítě a jejich aplikace: LAN / MAN / WAN. 2. aktualiz. vyd. Praha: Grada, 2003. ISBN 80-247-0545-1.
13. TIA Standard: Balanced Twisted-Pair Telecommunications Cabling and Components Standards. Innowave.com [online]. Arlington, VA, U.S.A.: Telecommunications industry association, 2009 [cit. 2017-04-06]. Dostupné z: <http://innovave.com/wp-content/uploads/2016/01/TIA-568-C.2.pdf>
14. LSZH and PVC cables. Black Box network services [online]. Hallbergmoos, Německo, 2009 [cit. 2017-04-06]. Dostupné z: <https://www.black-box.de/en-de/page/27275/Resources/Technical-Resources/Black-Box-Explains/Copper-Cable/lshz-and-pvc-cables/>
15. Rack IMG Stage Line MR-720. Muziker.cz [online]. 2017 [cit. 2017-04-13]. Dostupné z: <https://www.muziker.cz/img-stage-line-mr-720>
16. PANTŮČEK, Edmund. Poznatky z provádění kontrol elektrické instalace [online]. Praha: Schrack.cz, 2016, s. 29 [cit. 2017-04-06]. Dostupné z: [https://www.schrack.cz/fileadmin/f/cz/Bilder/Infodny\\_2016/Prezentace\\_Infodny/Nejcastejsi\\_chyby\\_v\\_elektroinstalacich\\_Pantucek.pdf](https://www.schrack.cz/fileadmin/f/cz/Bilder/Infodny_2016/Prezentace_Infodny/Nejcastejsi_chyby_v_elektroinstalacich_Pantucek.pdf)
17. Twisted pair. Wikipedia.org [online]. 2017 [cit. 2017-04-06]. Dostupné z: [https://en.wikipedia.org/wiki/Twisted\\_pair](https://en.wikipedia.org/wiki/Twisted_pair)
18. Voice Over IP - Per Call Bandwidth Consumption. Cisco.com [online]. 2016 [cit. 2017-04-06]. Dostupné z: <http://www.cisco.com/c/en/us/support/docs/voice/voice-quality/7934-bwidth-consume.html>
19. DECT. European Telecommunications Standards Institute [online]. 2017 [cit. 2017-04-13]. Dostupné z: <http://www.etsi.org/technologies-clusters/technologies/dect>
20. What is SaaS? Interoute.com [online]. 2017 [cit. 2017-04-06]. Dostupné z: <http://www.interoute.com/what-saas>
21. VDOLEČEK, František. Spolehlivost a technická diagnostika [online]. Brno: VUT v Brně - Fakulta strojního inženýrství - Ústav automatizace a informatiky, 2002, s. 8-9 [cit. 2017-04-06]. Dostupné z: <http://autnt.fme.vutbr.cz/lab/a1-731a/FSD.pdf>
22. Patriot Flare 120GB - Srovnání cen. Heureka.cz [online]. 2017 [cit. 2017-04-06]. Dostupné z: [https://pevne-disky.heureka.cz/patriot-flare-120gb-2\\_5-sata-ssd-pfl120gs25ssdr/](https://pevne-disky.heureka.cz/patriot-flare-120gb-2_5-sata-ssd-pfl120gs25ssdr/)

23. OCZ Vector 150: v testu výdrže jej umučíme k smrti. Svethardware.cz [online]. Brno, 2015 [cit. 2017-04-06]. Dostupné z: <http://www.svethardware.cz/recenze-ocz-vector-150-v-testu-vydrze-jej-umucime-k-smrti/40050>
24. PIR detektor: skvělý sluha, ale zlý pán. Vyvoj.hw.cz: Profesionální elektronika [online]. 2013 [cit. 2017-04-06]. Dostupné z: <http://vyvoj.hw.cz/automatizace/pir-cidlo-skvely-sluha-ale-zly-pan.html>
25. Výsledky 3. ročníku soutěže Vychytávka s JABLOTRON 100. Jablotron [online]. Jablonec nad Nisou, 2016 [cit. 2017-04-06]. Dostupné z: <http://www.jablotron.com/cz/pro-montery-alarmu/sekce/aktuality/vysledky-3-rocniku-souteze-vychytavka-s-jablotron-100/>
26. SDI a ti druzí, aneb na čem frčí profíci: SDI a jeho varianty. TV Freak [online]. Brno: OxyOnline, 2011 [cit. 2017-04-06]. Dostupné z: <http://www.tvfreak.cz/sdi-a-ti-druzi-aneb-na-cem-frci-profici/4521-2>
27. H.265/HEVC vs H.264/AVC: 50% bit rate savings verified. BBC - Research and Development [online]. London: BBC, 2017 [cit. 2017-04-06]. Dostupné z: <http://www.bbc.co.uk/rd/blog/2016-01-h-dot-265-slash-hevc-vs-h-dot-264-slash-avc-50-percent-bit-rate-savings-verified>
28. ASRock Debuts AM4 Motherboards With 5 Gigabit LAN. Tom's Hardware [online]. 2017 [cit. 2017-04-06]. Dostupné z: <http://www.tomshardware.com/news/asrock-amd-am4-10g-ryzen,33366.html>
29. HIKVISION DS-2CD2342WD-I (2.8mm). Viakom [online]. 2017 [cit. 2017-04-06]. Dostupné z: <https://www.viakom.cz/hikvision-ds-2cd2342wd-i-2-8mm/product-970>
30. HIKVISION DS-2CD4125FWD-IZ (2.8-12mm). Viakom [online]. 2017 [cit. 2017-04-06]. Dostupné z: <https://www.viakom.cz/hikvision-ds-2cd4125fwd-iz-2-8-12mm/product-1087>
31. Bezpečnostní inženýrství - Detektory požárů a senzory plynů. Vysoká škola chemicko-technologická v Praze [online]. Praha, 2017 [cit. 2017-04-06]. Dostupné z: [http://uchi.vscht.cz/uploads/pedagogika/bezpecnostni\\_inzenyrstvi/09.BI.Senzory.pdf](http://uchi.vscht.cz/uploads/pedagogika/bezpecnostni_inzenyrstvi/09.BI.Senzory.pdf)
32. Is it a good idea to build your own fluorescent video lights? Fixing a video [online]. 2015 [cit. 2017-04-09]. Dostupné z: <http://fixingyourvideo.com/wf-kino>

33. Světelná účinnost zdrojů světla (žárovky, kompaktní zářivky, výbojky a dalších). Stavebnictvi3000.cz: nejvíce informací o stavebnictví v ČR [online]. 2008 [cit. 2017-04-09]. Dostupné z: <http://www.stavebnictvi3000.cz/clanky/zarovka-usporna-zarovka-mnozstvi-svetla/>
34. SMD LED module. Wikipedia.org [online]. 2017 [cit. 2017-04-09]. Dostupné z: [https://en.wikipedia.org/wiki/SMD\\_LED\\_Module](https://en.wikipedia.org/wiki/SMD_LED_Module)
35. GAINES, Kristi S.; CURRY, Zane D. The inclusive classroom: The effects of color on learning and behavior. Journal of Family & Consumer Sciences Education, 2011, 29.1: 46-57.
36. DVOŘÁK, Petr. Vliv modrého světla na lidský organismus [online]. Vysoké učení technické v Brně. Fakulta elektrotechniky a komunikačních technologií, 2016 [cit. 2017-04-06]. Dostupné z: <http://hdl.handle.net/11012/60483>. Bakalářská práce. Vysoké učení technické v Brně. Fakulta elektrotechniky a komunikačních technologií. Ústav elektroenergetiky. Vedoucí práce Jaroslav Štěpánek.
37. Větrání škol: problémy vedou k nové vyhlášce. Smart Cities [online]. Praha, 2017 [cit. 2017-04-06]. Dostupné z: <http://www.scmagazine.cz/casopis/01-16/vetrani-skol-problemy-vedou-k-nove-vyhlasce?locale=cs>
38. Hygienické parametry vnitřního prostředí ve třídě. ASB-portal.cz: odborný stavební portál [online]. Praha: Jaga Media, 2016 [cit. 2017-04-06]. Dostupné z: <https://www.asb-portal.cz/tzb/vetrani-a-klimatizace/hygienicke-parametry-vnitriho-prostredi-ve-tride>
39. Wikileaks Unveils 'Vault 7': "The Largest Ever Publication Of Confidential CIA Documents"; Another Snowden Emerges. Ron Paul - Liberty report [online]. 2017 [cit. 2017-04-06]. Dostupné z: <http://www.ronpaullibertyreport.com/archives/wikileaks-unveils-vault-7-the-largest-ever-publication-of-confidential-cia-documents-another-snowden-emerges>
40. Vault7 - Home. Wikileaks [online]. 2017 [cit. 2017-04-06]. Dostupné z: <https://wikileaks.org/ciav7p1/>
41. All current and historical changelogs. Mikrotik.com [online]. Riga, LV, 2017 [cit. 2017-04-06]. Dostupné z: <https://mikrotik.com/download/changelogs>

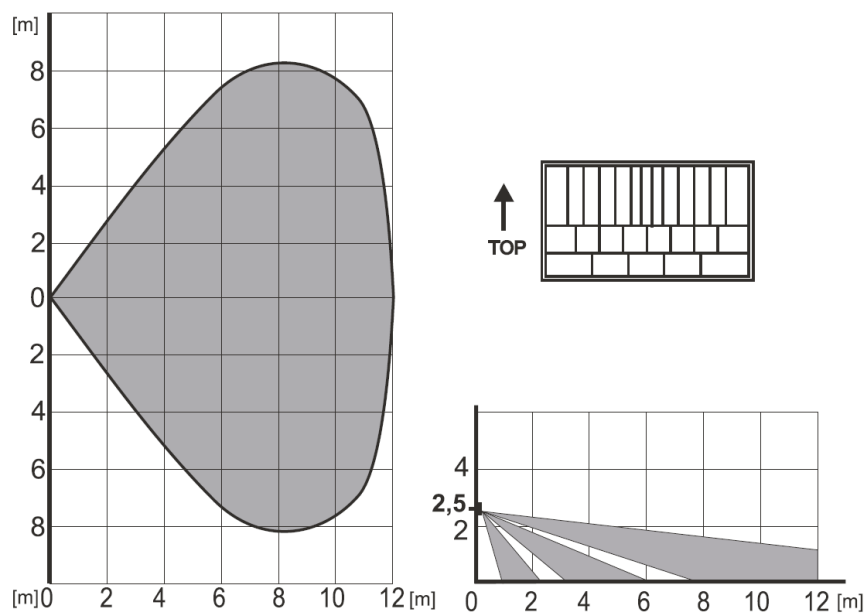
42. The Wikileaks Vault 7 Leak – What We Know So Far. Cisco.com [online]. 2017 [cit. 2017-04-06]. Dostupné z: <http://blogs.cisco.com/security/the-wikileaks-vault-7-leak-what-we-know-so-far>
43. Mapa pokrytí. IoT portál: brána do světa internetu věcí [online]. 2017 [cit. 2017-04-06]. Dostupné z: <https://www.iot-portal.cz/mapa-pokryti/>

# **Přílohy**

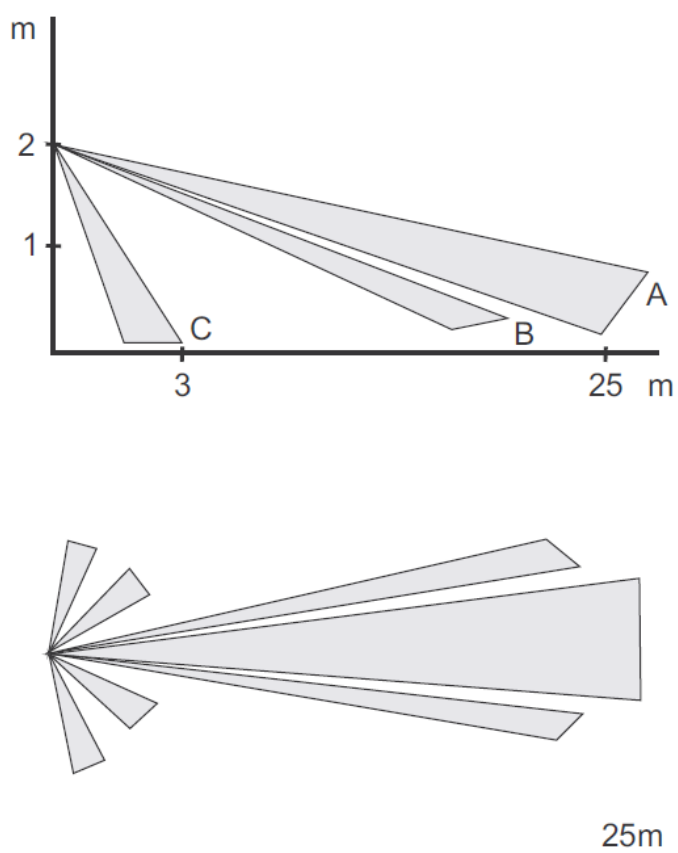


## Příloha č. 1

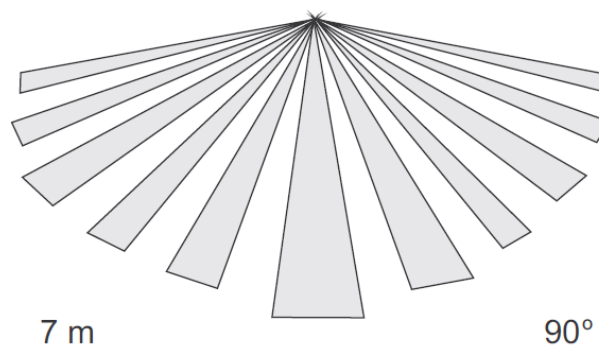
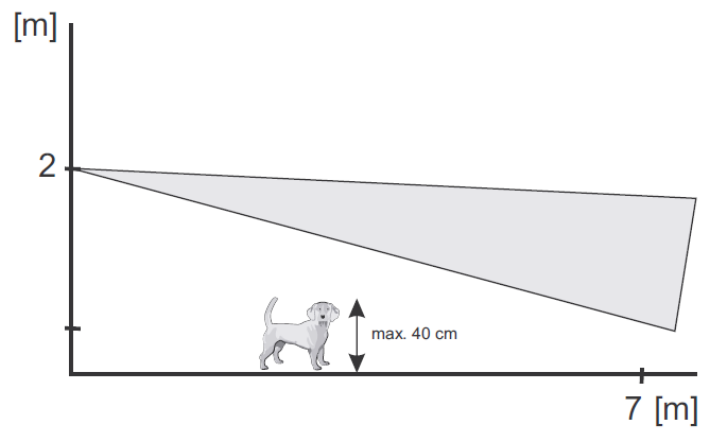
### Směrové detekční charakteristiky PIR detektorů



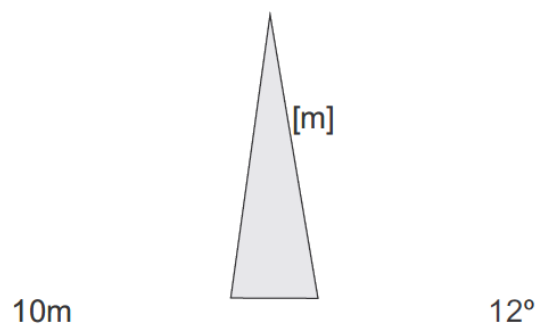
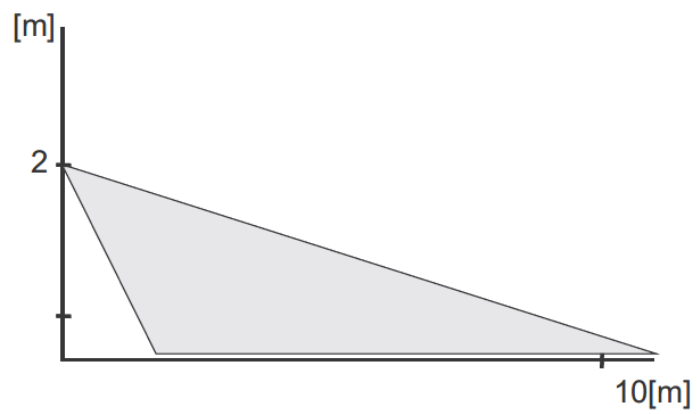
Ilustrace 6: Standardní chodbová čočka - JA-110P



Ilustrace 7: Čočka pro dlouhé chodby (JS-7904)

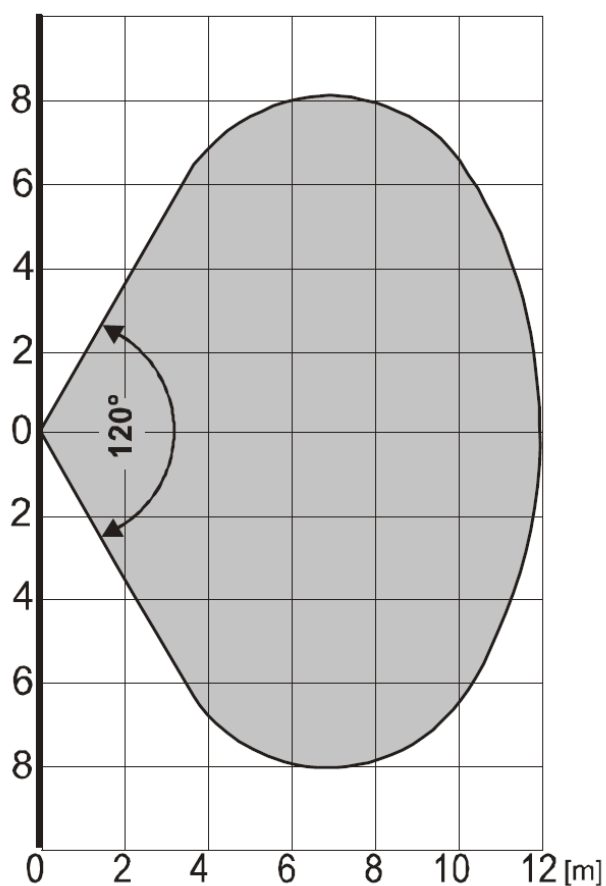


Ilustrace 8: Zvířecí čočka (JS-7910)

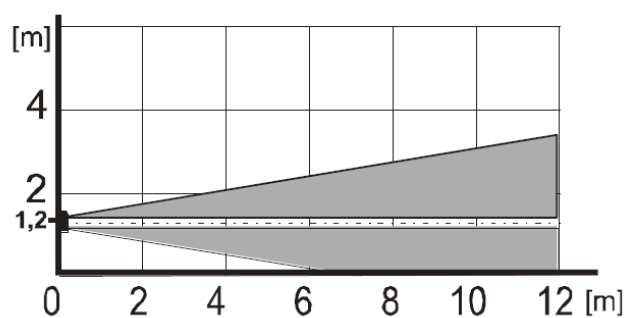


Ilustrace 9: Záclonová čočka (JS-7902)

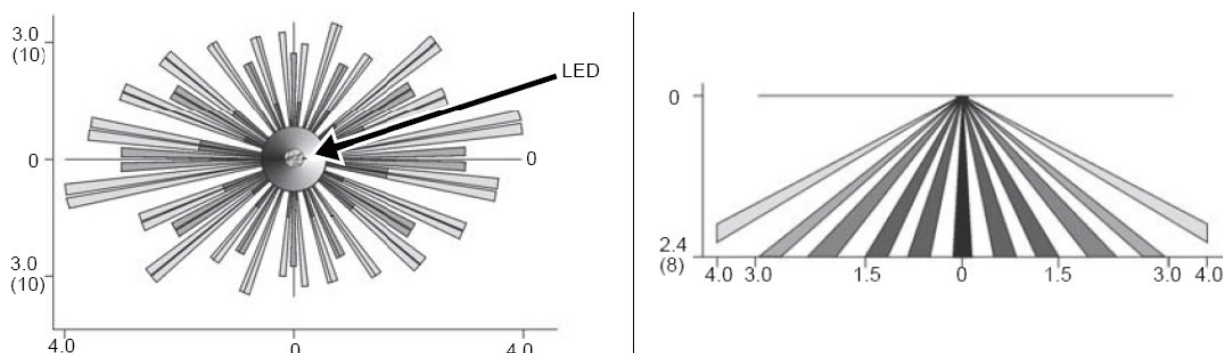
## Pohled shora



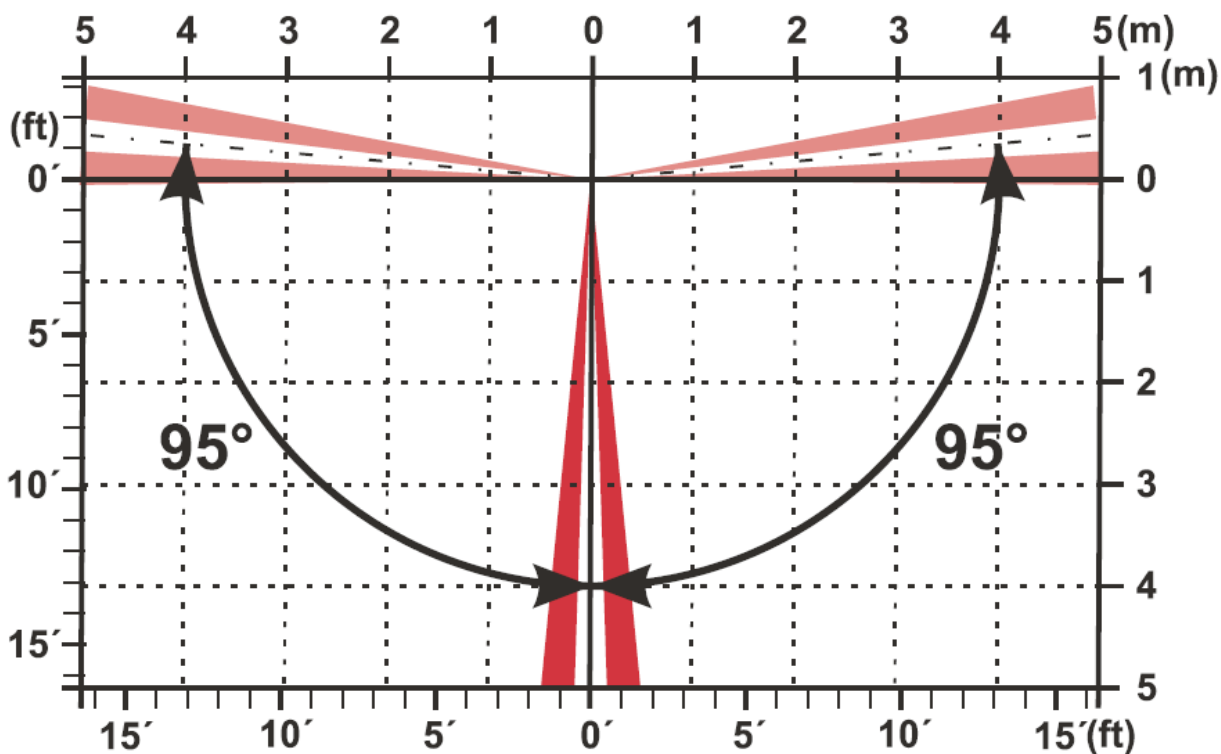
## Pohled z boku



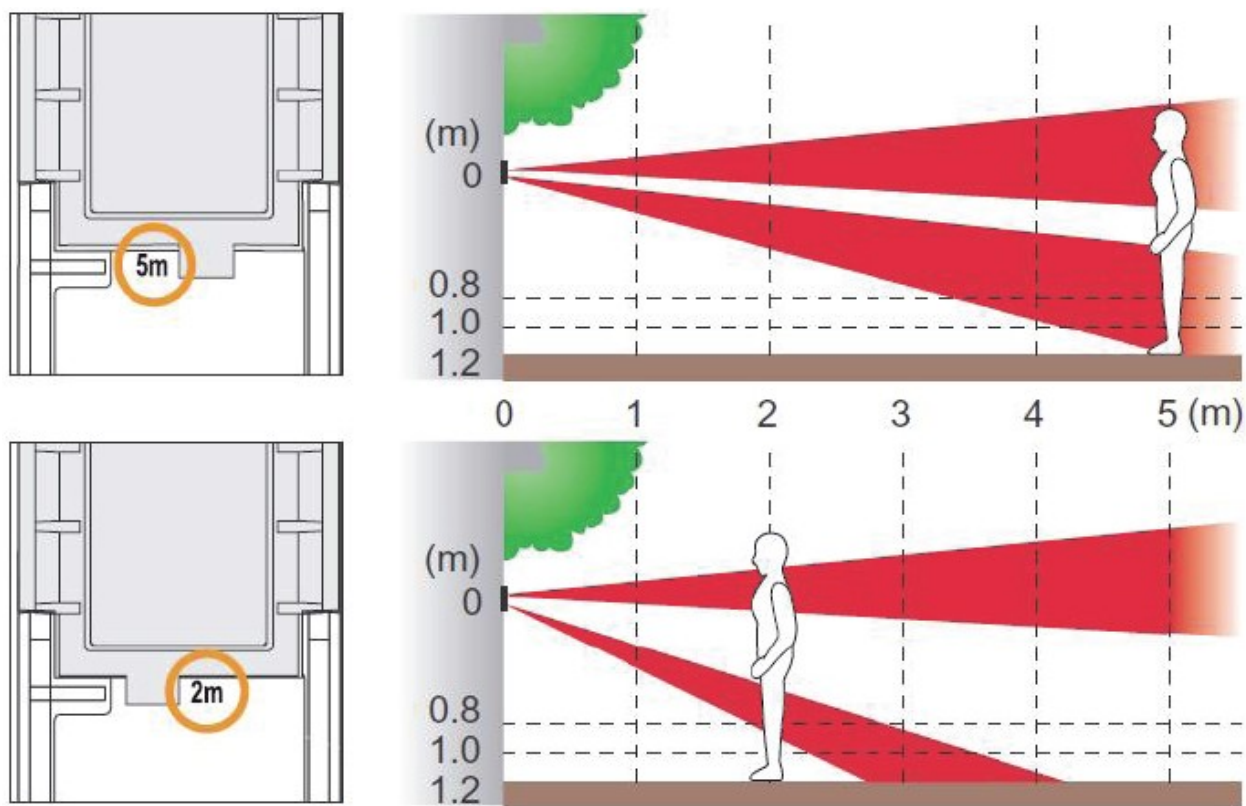
Ilustrace 10: Vnitřní dvouzónový detektor (JA-186P)



Ilustrace 11: Stropní detektor Paradox (Paradome)



Ilustrace 12: Venkovní dvouzónový záclonový detektor JA-157P - nastavení směru detekce



Ilustrace 13: Venkovní dvouzónový záclonový detektor JA-157P - možnost volby dvou detekčních vzdáleností

## Příloha č. 2

### **Metodické doporučení k bezpečnosti dětí, žáků a studentů ve školách a školských zařízeních – Minimální standard bezpečnosti**

Ministerstvo školství, mládeže a tělovýchovy (dále jen „ministerstvo“) vydává toto metodické doporučení k bezpečnosti dětí, žáků a studentů ve školách a školských zařízeních – Minimální standard bezpečnosti - s cílem podat přehled doporučených opatření k zajištění bezpečnosti a ochrany zdraví dětí, žáků a studentů v budovách škol a školských zařízení a v areálech škol a školských zařízení k nim náležejících.

Metodické doporučení bylo zpracováno jako jedno z opatření ministerstva, které bylo přijato na základě úkolu (uvedeného pod bodem č. 38 záznamu jednání s názvem Zadání vlády k tragické události ve Žďáru nad Sázavou) ze 40. schůze vlády České republiky ze dne 15. října 2014. Usnesení vlády č. 1015 dne 8. prosince 2014 podpořilo tvorbu metodického pokynu. Metodické doporučení se opírá i o závěry z tematické zprávy České školní inspekce (inspekční šetření probíhalo ve dnech 20. 10. 2014 – 13. 11. 2014) s názvem Bezpečnost ve školách a školských zařízeních č. j.: ČŠIG-4027/14-G2 z měsíce listopadu 2014.

V současnosti neexistuje právní předpis, který by na jednom místě shrnoval základní a konkrétní opatření na zajištění bezpečnosti dětí, žáků a studentů ve školách a školských zařízeních, zapsaných do školského rejstříku, neboť část této problematiky spadá do působnosti jiných ústředních orgánů státní správy.

Minimální standard bezpečnosti mohou využít školy i školská zařízení při jednání se zřizovateli, a to s ohledem na nutná opatření vyplývající z jejich potřeb, charakteru provozu a z místních podmínek.

Ministerstvo upozorňuje, že toto metodické doporučení bude aktualizováno poté, co nabude účinnosti připravovaná vyhláška o opatřeních k zajištění bezpečnosti a ochrany zdraví dětí, žáků a studentů ve školách a školských zařízeních; k jejímu vydání je ministerstvo zmocněno v ustanovení § 29 odst. 2 zákona č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon).

Za účelem dostatečného zajištění ochrany budov ministerstvo vyhlásí dotační program „Podpora zabezpečení škol a školských zařízení“. Tento dotační program bude zveřejněn na webových stránkách ministerstva.

V Praze dne 20. února 2015

Mgr. Jaroslav Fidrmuc  
náměstek ministra pro vzdělávání

**Metodické doporučení  
k bezpečnosti dětí, žáků a studentů ve školách a školských zařízeních –  
Minimální standard bezpečnosti**

Č.j.: MSMT-1981/2015-1

**Minimální standard bezpečnosti** právnické osoby vykonávající činnost školy nebo školského zařízení (dále jen „škola“) zahrnuje opatření prostorová, organizačně-technická, personální a opatření v oblasti zpracované dokumentace. Jeho význam je metodický, ne normativní. Mimo tato opatření, která směřují především k zajištění fyzické bezpečnosti dětí, žáků a studentů (dále jen „žáků“), má škola na zřeteli rovněž psychické bezpečí žáků, a proto opatření k zajištění fyzické bezpečnosti ve škole nesmí snížit psychické bezpečí a komfort žáků.

Problematiku zajištění minimálního standardu bezpečnosti je třeba vnímat v těchto rovinách:

1. **Prevenčí předcházet mimořádným událostem** (technická opatření, poučení zaměstnanců a žáků, nácvik řešení mimořádných událostí dle specifických podmínek škol, přehled o cizích osobách v objektu, spolupráce se složkami Integrovaného záchranného systému,...).
2. **Účinně a efektivně reagovat na mimořádnou událost**, která nastala a snažit se o omezení škod na životech a zdraví zaměstnanců i žáků.
3. **Vyhodnotit mimořádnou událost a přijmout opatření**, aby se nemohla opakovat ze stejných příčin i v budoucnu).

**1. Prostorová a organizačně-technická opatření**

- Škola určí a využívá pro vstup žáků, zaměstnanců a cizích osob (návštěv, kontrol, atp.) zpravidla pouze jeden vchod, který je zabezpečen proti vniknutí cizích osob a vstup do něj je kontrolován (monitorován); ostatní možné vstupy do budov jsou zabezpečeny (nesmí však bránit bezpečnému úniku osob v případě požáru) a užívají se případně jako vstupy pro zaměstnance nebo pro cizí osoby, které se účastní dalšího vzdělávání v jiných prostorách školy (např. odborný výcvik, kurzy, školení, atp.), přičemž i v tomto případě má škola zajištěnu kontrolu vstupu. Školy pavilonové dispozice přijímají tato opatření přiměřeně podle svých podmínek.
- Škola vpouští cizí osoby do prostor školy až po ověření účelu jejich vstupu do budovy (doprovod žáka, návštěva pedagoga či ředitele školy, apod.); to platí též v případě vjezdu dopravním prostředkem do areálu školy. Vstupy a vjezdy do areálu školy jsou kontrolovány (monitorovány).
- Škola má uzamykatelné vstupy do budov i dalších prostor v areálu školy (např. školní zahrady, školního dvora, parkoviště, apod.), má zabezpečená okna a dveře proti volnému vniknutí osob.

Na začátku, v průběhu dne i na jeho konci škola vstupy zabezpečí (klíčový režim musí být vyřešen tak, aby byly únikové cesty trvale volné a umožňovaly bezpečný únik z budovy).

- Škola zamezuje nepovolaným osobám přístup do dalších prostor, budov i areálu školy, které nejsou určeny pro poskytování vzdělávání (např. sklepy, půdy, sklady, kotelny, apod.), s výjimkou specifických, zvláště provozních případů (revize, kontroly, prohlídky, stavební úpravy, apod.).
- Škola má provedenu úpravu zeleně pro zvýšení přehlednosti prostor v okolí přístupových cest i další okolní terénní úpravy.
- Škola má ve svém areálu funkční venkovní osvětlení (nejlépe ovládané pohybovým čidlem) přístupových cest, a to i v době mimo provoz školy.

**Ke splnění těchto požadavků se předpokládá zajištění a provedení například:**

- bezpečnostních zámků,
- závor,
- oplocení,
- osvětlení,
- drobných stavebních a terénních úprav.

## **2. Personální opatření**

- Škola zajišťuje průběžný dohled nad žáky ve všech prostorách, a to od okamžiku vstupu do prostor školy po celý průběh výchovně-vzdělávacího procesu i po jeho ukončení až po dobu opuštění budovy či areálu školy. O zajištění náležitého dohledu rozhoduje ředitel školy. Vychází přitom z konkrétních podmínek a přihlíží zejména k charakteru vykonávané činnosti, věku žáků a jejich rozumovému rozvoji (vypětosti), dopravním a jiným rizikům. Ředitel školy zpravidla pověřuje dohledem pedagogického pracovníka, stanoví rozvrh dohledu nad žáky a vyvěsí ho na takovém místě, aby bylo možné při kontrolní činnosti snadno rozpoznat, který pedagogický pracovník dohled vykonává.
- Škola má zajištěnou vzájemnou zastupitelnost pedagogických či nepedagogických pracovníků vykonávajících dohled nad žáky.
- Škola zajišťuje dohled nad žáky i při akcích souvisejících se vzděláváním, které jsou realizovány mimo školu. Při pravidelném využívání budov či místností (např. tělocvičen obcí), které nejsou v majetku školy, je nutné vyžadovat od pronajímatele ujištění o bezpečném stavu budovy či místnosti (např. doložením revizních zpráv se závěrem „schopno bezpečného provozu“).
- Škola v případě avízovaného nebezpečí využívá možnosti posílení ostrahu budovy městskou či státní policií, případně hlídkami bezpečnostních agentur (dle místních zvyklostí).

**Ke splnění těchto požadavků se předpokládá zajištění:**

- finančních prostředků pro vrátné nebo jiné osoby vykonávající ostrahu školy,
- finančních prostředků na nárůst pracovních úvazků na zajištění dohledu.

Jednou z možností, jak získat finanční prostředky pro zajištění činnosti vrátného, je vytvoření tzv. společensky účelného pracovního místa (za stanovených kritérií pro výběr zaměstnance) na základě dohody s Úřadem práce České republiky. V rámci systému aktivní politiky zaměstnanosti tak může škola čerpat finanční příspěvek na úhradu mzdových nákladů.

### 3. Vnitřní předpisy, dokumentace školy

- Škola, ve spolupráci s osobami odborně způsobilými v prevenci rizik a osobami odborně způsobilými v oblasti požární ochrany, analyzuje rizika podle podmínek a charakteru své činnosti a má zpracovány dokumenty pro mimořádné události (např. neoprávněné vniknutí do objektu, přítomnost neznámého nebo nebezpečného předmětu nebo látky ve škole, útok vedený zvenčí či zevnitř, braní rukojmí, vandalismus, šikana,...).
- Škola má zajištěny mechanismy ověřování účinnosti výše uvedené dokumentace, včetně periodických zkoušek technických prostředků a zařízení a spolupracuje se složkami integrovaného záchranného systému a s orgány místní správy.
- Škola má v pracovním řádu, školním řádu/vnitřním řádu a v dokumentaci podle jiných právních předpisů, upraveny i další zvláštní povinnosti zaměstnanců, např. povinnosti a postupy při zajišťování dohledu, povinnost informovat zaměstnavatele o vzniku mimořádných událostí, povinnost důsledně dbát na účinnost technických a jiných prostředků chránících bezpečnost budov, povinnost seznamovat zaměstnance a žáky školy s opatřeními zajišťujícími bezpečnost a ochranu zdraví (na začátku školního roku, průběžné opakování dle vyhodnocených rizik, povinnost provedení záznamu o poučení).
- Škola má vymezen formální rámec bezpečnosti a ochrany zdraví, včetně pojmenování nebezpečí, rizik možného ohrožení života a zdraví žáků, spolu s přijetím adekvátních opatření. Škola seznamuje žáky a zaměstnance s ustanoveními předpisů a pokynů k zajištění bezpečnosti a ochrany zdraví, včetně pojmenování nebezpečí, rizik možného ohrožení života a zdraví, pokud se vztahují k příslušné činnosti, akci nebo pracovišti a průběžně také s ustanoveními školního nebo vnitřního řádu, řádů dílen, laboratoří, odborných pracoven, sportovních zařízení, tělocvičen, hřišť a jiných pracovišť a s dalšími opatřeními, jež mohou mít bezpečnostně preventivní význam při uplatňování základních pravidel bezpečného chování (např. cizí osoby ve školách, technické zabezpečení vstupu do budov, dohled pedagogických pracovníků, způsob příchodu a odchodu, zabezpečovací prvky ve škole). Škola má popsány a uplatňuje účelné způsoby chování v situacích ohrožujících zdraví, má stanovena zvláštní pravidla při některých činnostech – tělesné výchově, plavání, koupání, lyžařském výcviku,



sportovně-turistickém kurzu, soutěžích, přehlídkách, výletech, škole v přírodě, zahraničních výjezdech, apod.

- Škola informuje zákonné zástupce žáků o vydání a obsahu školního nebo vnitřního řádu.

Od výše uvedeného minimálního standardu by se měla škola odchýlit jen v nezbytně nutných a odůvodněných případech, budou-li to vyžadovat místní podmínky. V případě jakýchkoli odchylek je však třeba přijmout taková opatření, aby byla bezpečnost a ochrana zdraví žáků i zaměstnanců zajištěna jinými konkrétními způsoby, aniž by byly v rozporu s výše uvedenými principy. Současně musí škola plnit povinnosti, které jí vyplývají z právních předpisů.

Školy mají možnost zajistit bezpečnost osob v areálu školy také dalšími, např. technickými prostředky, které jdou nad rámec výše vymezených minimálních požadavků (např. vstup na čipy, turnikety, kamerový systém, čipy, elektronický vrátný, alarm s tísňovými tlačítky napojený na dispečink, apod.); tyto technické prostředky však nemohou plně nahradit dohled prováděný fyzickou osobou, a jde-li o kamerový systém, bere škola před jeho zavedením v úvahu i ochranu soukromí žáků i zaměstnanců školy.

Školy při eliminaci bezpečnostních rizik spolupracují se zřizovatelem, se zákonnými zástupci žáků, zletilými žáky, policií, složkami integrovaného záchranného systému a se školskou radou.

Další předpisy související se zabezpečením budov:

#### **Mechanické zábrany**

- ČSN EN 1627 Dveře, okna, lehké obvodové pláště, mříže, okenice.  
- Požadavky a klasifikace, odolnost proti násilnému vniknutí (požadavky na odolnost dveří a oken včetně kování, cylindrických vložek a skel).

#### **Kamerové systémy**

- ČSN EN 62676 (řada) Dohledové videosystémy pro použití v bezpečnostních aplikacích

#### **Poplachové systémy (alarmy)**

- ČSN EN 50131–1 (ed. 2) Poplachové zabezpečovací a tísňové systémy
- ČSN EN 50132-5 Poplachové systémy - CCTV sledovací systémy pro použití v bezpečnostních aplikacích - Část 7: Pokyny pro aplikaci

#### **Systémy kontroly vstupu**

- ČSN EN 60839-11-1 Poplachové a elektronické bezpečnostní systémy - Část 11-1: Elektronické systémy kontroly vstupu - Požadavky na systém a komponenty.
- ČSN EN 50133-1 Poplachové systémy – Systémy kontroly přístupu pro použití při bezpečnostních aplikacích.

#### **Doporučené kvalifikační požadavky na vrátného**

Vrátný by měl být kvalifikován pro bezpečnostní činnosti. Nejblíže je to kvalifikace Strážný (kód: 68-008-E) z národní soustavy kvalifikací.

<http://www.narodnikvalifikace.cz/kvalifikace-315-Strazny>

#### **Ochrana soukromí při nasazení kamerových systémů**

- Zákon 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů
- Vyjádření a doporučení Úřadu pro ochranu osobních údajů k možnosti instalovat kamerový systém v prostorách školy ze dne 12. března 2007  
[https://www.uouu.cz/files/vyjadreni\\_a\\_doporuceni\\_uouu.pdf](https://www.uouu.cz/files/vyjadreni_a_doporuceni_uouu.pdf)

## Příloha č. 3

### Vyjádření a doporučení ÚOOÚ k možnosti instalovat kamerový systém v prostorách školy

Zpracováno 12. března 2007

(Vydává se v návaznosti na publikované vyjádření odboru legislativního a právního Ministerstva školství, mládeže a tělovýchovy ČR ze dne 6.12. 2006.<sup>1)</sup>)

Základní přístupová kritéria Úřadu pro ochranu osobních údajů (dále jen „Úřad“) lze shrnout do těchto zásad, které je nutno v konkrétním případě vždy posoudit dříve, nežli se učiní rozhodnutí o instalaci kamerového systému:

- Ochrana práva jednotlivce by měla být vždy zohledněna ve vztahu k zájmům, provozovatele školy nebo školského zařízení (dále jen „škola“), který musí vykonávat svá práva a povinnosti způsobem co nejméně zasahujícím do soukromí, a to nejen zaměstnanců a žáků, ale i dalších osob.
- Škole musí být zřejmý velmi závažný důvod nebo vážná příčina, pro který je kamerový systém instalován a který neumožňuje použít jiný, méně invazivní prostředek zasahující do soukromí osob pohybujících se ve sledovaném prostoru. Přitom je třeba zdůraznit, že kamerový systém nelze nasazovat a ani následně využívat za účelem sledování fyzických osob – žáků, učitelů nebo zaměstnanců školy, ale pouze pro legitimní účely jako je například ochrana majetku.
- Musejí být dána jasná pravidla pro přístup jen vymezeného okruhu osob k systému a v něm uchovávaným záznamům nebo k jeho jednotlivým částem, včetně oprávnění manipulovat se sledovacími zařízeními nebo jejich režim upravovat.
- Rovněž je nezbytné řešit zvláštní režim přístupu oprávněných osob k uchovávaným záznamům, to znamená, jak osob pověřených správcem pro nahlížení do záznamů, tak osob, které využijí svého práva přístupu k zaznamenaným údajům o nich.
- Musí být stanovena doba uchovávání záznamů, která nepřesáhne dobu potřebnou k tomu, aby incident zaznamenaný kamerou bylo možno zjistit dodatečnými prostředky a předat k vyšetření příslušným orgánům. Přitom doba uchování by při běžném provozu systému neměla přesáhnout délku několika dnů s přihlédnutím k možným odchylkám jednotlivých záznamů pořizovaných například během prázdnin.
- Před spuštěním systému by měl být vypracován projekt rozmístění kamer a instalace jednotlivých sledovacích a záznamových zařízení včetně stanovení režimu (časového) pro provoz jednotlivých snímacích stanišť, který by měl být kritériem pro posouzení funkčnosti systému i z pohledu zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon“).

Pokud se shrnou shora uvedené podmínky a předpoklady pro zákonný rámec provozování kamerových systémů, lze v zásadě s přihlédnutím k současným postojům Úřadu, jejichž snahou je omezit provozování kamerových systémů ve školách jen na nezbytně nutnou míru, souhlasit s větší částí stanoviska MŠMT v tom směru, že:

- Skutečnost, že neexistuje zvláštní právní úprava podmínek pro provozování kamerových systémů neznámá, že škola při splnění svých zákonných povinností správce osobních údajů nemůže rozhodnutí o instalaci kamerového systému se záznamem učinit.
- Pokud se škola k tomuto kroku rozhodne, ocitá se toto zpracování v režimu zákona a musí proto splnit zde uváděné zákonné podmínky:
  - Učinit oznámení o zpracování podle § 16 zákona.

- Zpracovávat osobní údaje pouze se souhlasem subjektu údajů podle § 5 odst. 2, pokud škola neprokáže kvalifikovaný důvod, který by ji opravňoval ke zpracování osobních údajů bez souhlasu.
- Provozovat systém tak, aby bylo soukromí osob s ohledem na jejich právo podle § 10 zákona narušováno minimálně (posuzováno je např. i umístění kamer, úhel záběru, zobrazovací schopnost apod.).
- Informovat monitorované osoby o instalaci a provozu systému podle § 11 zákona.
- Přijmout bezpečnostní opatření pro provozování systému a ochranu zpracovávaných informací podle § 13 zákona a stanovit přiměřenou dobu pro uchovávání záznamů podle § 5 odst. 1 písm. e).
- Respektovat podmínky zvláštních právních předpisů upravujících možnosti sledování osob (zejména § 316 odst. 2 zákoníku práce).

#### **Závěr:**

Nad rámec výše uvedeného doporučení lze uvést:

**Záměrem tohoto vyjádření je odstranit přetrvávající rozdíly v přístupu k otázce, v jakých prostorách žáci i zaměstnanci školy, uplatňují své právo na soukromí.**

**V tomto směru se odkazuje na judikaturu Evropského soudu pro lidská práva (ESLP)<sup>2</sup>, podle které je nutno pod pojmem soukromí člověka rozumět právo každého člověka na vytváření a rozvíjení vztahu s dalšími lidskými bytostmi, a to i na pracovišti (a lze tedy dovodit, že i v prostorách, kde jsou žáci vzdělaváni) . Dle soudu není dost dobře možné přesně oddělit soukromý a profesionální život, neboť právě v rámci svých pracovních aktivit má většina lidí největší příležitost navazovat a rozvíjet vztahy s vnějším okolím, a proto právo na respektování soukromého života zahrnuje i právo na respektování soukromí v zaměstnání (viz např. rozhodnutí ve věci Niemietz v. Německo z roku 1992).**

#### Poznámka:

<sup>1</sup> Plné znění dokumentu „Vyjádření odboru legislativního a právního MŠMT k otázce používání kamer ve školách“ ze dne 6. 12. 2006 je k dispozici na internetové adrese [http://www.ucitelskenoviny.cz/nastenka\\_clanek.php?odkaz=kamery.html](http://www.ucitelskenoviny.cz/nastenka_clanek.php?odkaz=kamery.html) .

<sup>2</sup>Více informací o ESLP je k dispozici na internetové adrese [www.echr.coe.int](http://www.echr.coe.int) .