BEZPEČNOSTNÍ TECHNOLOGIE A SYSTÉMY

Jaromír Kyncl

Kvalitativní a cenově dostupné zajištění bezpečnosti objektu je dnes nedílnou součástí podnikatelské strategie nejenom většiny veřejných i soukromých organizací všech velikostí, typů a forem, ale také jednotlivců, rodin a jejich zájmových subjektů. Výrobci, dodavatelé i špičkoví poskytovatelé bezpečnostních služeb nabízí při budování kvalitního bezpečnostního systému nejmodernější soudobé bezpečnostní technologie, při procesu vlastní realizace je však nutno vzít v potaz mnoho technologických a ekonomických faktorů. V úvahu je také nezbytné vzít konkurenční vztahy výrobců bezpečnostních technologií (BT).

Jinými slovy se každý snaží dělat všechno a současně bojuje o zákazníka – snaží se mu vysvětlit, proč právě jeho portfolio výrobků je to nejlepší. Aby si lépe uchránil těžce získané zákazníky, nedovolí jiným výrobcům, aby se mohli připojit k původnímu zařízení a podporují pouze své produkty. To má za následek omezené možnosti výběru pro zákazníka, a tím i zpomalení rozvoje odvětví (poplachových zabezpečovacích a tísňových systémů). Do jisté míry tuto situaci řeší společnosti, které vytvářejí nadstavbové integrační softwary. Zástupci těchto společností kontaktují výrobce produktů PZTS, CCTV, EPS, MZS a snaží se jim vysvětlit, že nejsou jejich konkurenti, ale naopak, pokud jim někteří výrobci zpřístupní komunikační kódy jednotlivých zařízení, získají tak možnost propojit své výrobky s dalšími systémy a mohou zákazníkovi nabídnout komplexní systém s plnohodnotnou integrací nejenom s PZTS, CCTV, EPS, MZS, ale například i se systémy platebních terminálů nebo inteligentní elektroinstalací."[1]

[1] HUCAN, Jiří; MIGDA Josef: *Inovace v oblasti PZTS a perimetrických systémů.* In: NOVÁŠ, Luděk: Bezpečnostní technologie, systémy management I. VeRBum – Ra... Hradec Králové. Zlín 2011. ISBN 978-80-87500-05-7. Str. 100.

Tato citace vystihuje pouze jeden z aspektů konkurenčního boje výrobců. Není bez zajímavosti, že propojení různých systémů a plnohodnotná integrace umožňuje používat pouze jedno uživatelské rozhraní a zákazník tak získává možnost rozšířit svůj bezpečnostní systém volitelně podle funkčních vlastností a momentální potřeby, nikoli pouze podle omezené řady produktů jednoho výrobce či dodavatele. Neustálý vývoj bezpečnostních systémů rozšiřuje možnosti jejich využití. Kromě účelu ochrany osob a majetku se jejich příslušné moduly sofistikovaněji zapojují jako prostředek požární signalizace, protipožární ochrany, lékařského monitoringu, hlášení nouzových situací ve výtazích nebo evakuačních procesů. Díky integraci všech bezpečnostních prvků a moderním komunikačním metodám pak mohou mít uživatelé jistotu, že se nezbytné informace dostanou včas na místo určení.

6.1 Poplachový zabezpečovací a tísňový systém (PZTS)

Jaromír Kyncl

Poplachový zabezpečovací a tísňový systém (PZTS), dříve nazývaný elektrická zabezpečovací signalizace (EZS), představuje komplexní soubor technických prostředků, jejichž prostřednictvím je řešena ochrana proti neoprávněnému vstupu do objektu. Neoprávněný vstup nepovolaných osob je včas rozpoznán a zároveň signalizován, čímž systém eliminuje případné škody. Systém PZTS tvoří ústředna, ovládací klávesnice, detektory a koncová zařízení. Tento systém lze realizovat jako nezávislou aplikaci nebo jako součást systémů v rámci sjednocení dalších systémů (např. CCTV, perimetrické ochrany, EKV).

V dnešní době, charakteristické stoupající kriminalitou, je potřeba chránit sebe i majetek vyšší, než byla v minulosti. Policejní statistiky dlouhodobě uvádějí objasněnost případů vloupání kolem 20 %. Svůj podíl na objasněnosti a hlavně samotném uskutečnění vloupání má i fakt, že PZTS je i přes svou finanční dostupnost stále málo využívaným způsobem zabezpečení. PZTS zvýší bezpečí objektu a jeho obyvatel a poskytuje významnou ochranu před ztrátou majetku, financí či důležitých dokumentů. V případě řádně instalovaného a certifikovaného systému PZTS poskytuje většina pojišťoven příznivější pojistné podmínky.

Zákazník si může vybrat mezi drátovou i bezdrátovou variantou, která je šetrná k interiérům při osazování již obydlených objektů. PZTS může střežit volný prostor kolem domu, plášť domu (okna, dveře) a v neposlední řadě

samotné vnitřní prostory. Používají se prostorová čidla pracující na různých principech, dveřní a okenní snímače a další prvky. Na narušení střežených prostor je okolí upozorněno vnitřní a vnější sirénou s majákem, je možné zaslání poplašné zprávy na předem zvolená telefonní čísla nebo na dohledové a poplachové přijímací centrum (dříve PCO). Poplachem systém reaguje i na pokus o zničení kteréhokoliv čidla, nebo na narušení prostoru silným zářením.

Rozdělení PTZS z hlediska prostorového zaměření:[2]

1. *perimetrická (obvodová) ochrana* – jedná se o technické prostředky, které signalizují narušení obvodu vyhrazeného území a prostor kolem střeženého objektu; obvod objektu tvoří jeho katastrální hranice, které jsou vymezené přírodními nebo umělými bariérami (vodní toky, zdi, ploty apod.);

2. *plášťová ochrana* – jedná se o technické prostředky, které signalizují narušení pláště budovy; plášťová ochrana zabezpečuje vstup do všech stavebních otvorů objektu (dveře, okna, balkónová a střešní okna, vikýře, šachty apod.) a zabraňuje jejich narušení;

3. *prostorová ochrana* – zabezpečuje ochranu prostoru uvnitř chráněného objektu; potenciální pachatel již překonal plášťovou ochranu a vnikl do vnitřních prostor objektu, přičemž bezpečnostní systém reaguje převážně na pohyb pachatele a signalizuje jevy s charakterem nebezpečí v chráněném prostoru;

4. *předmětová ochrana* – signalizuje pokus o napadení nebo neoprávněnou manipulaci s chráněným předmětem; chráněným předmětem se rozumí umělecké předměty, klenoty a také úschovná místa (trezory), kde jsou uloženy cennosti, jejichž zcizení případně zneužití by způsobilo újmu subjektu, který je vlastní; předmětová ochrana je využívána např. v muzeích, galeriích, bankách;

5. *tísňová ochrana* – signalizuje ohrožení života nebo zdravotní problémy fyzických osob, které jsou napadeny či ohroženy působením přírodních živlů (požár, voda, plyn) nebo vystaveny mimořádné události, při níž je nutno objekt evakuovat (teroristický útok); signalizace je vyvolána manuálně (stisk-

[2] CAHLÍK, Marek: *Bezpečnostné a zabezpečovacie systémy*. In: IDB JOURNAL. Čís. 3/2012. Str. 27.

nutí tlačítka), definovaným způsobem manipulace (nášlapná tísňová lišta) automaticky (hlásič nehybnosti, signálem pro stav tzv. „mrtvý muž").

6.2 Elektrická požární signalizace (EPS)

Jaromír Kyncl

Elektrická požární signalizace je vyhrazené požárně bezpečnostní zařízení, které zajišťuje včasnou signalizaci pomocí hlásičů požáru. K detekci požáru používá automatické bodové hlásiče, IR hlásiče plamene, lineární hlásiče kouře, nasávací hlásiče či speciální hlásiče, určené například do výbušného prostředí. Signály z hlásičů požáru jsou přijímány ústřednou EPS. U ústředny je zajištěna stálá obsluha, která v případě požáru přivolá jednotku požární ochrany. Pokud není zajištěna 24 hodinová obsluha, musí být systém EPS připojen zařízením dálkového přenosu (ZDP) na centrální dohledový pult příslušného hasičského záchranného sboru (HZS). V takovém případě je zabezpečený objekt vybaven obslužným polem požární ochrany (OPPO) a klíčovým trezorem (KTPO), v němž je umístěn generální klíč k objektu. Pro lepší orientaci by měl být nad KTPO umístěn červený maják. Rozlišujeme několik druhů EPS:

a) *jednostupňové EPS* – mají jednu nebo více hlavních ústředen, na které jsou připojeny samočinné a tlačítkové hlásiče požáru; na ústřednu jsou napojena ovládací a doplňující zařízení; jednostupňové EPS nemají vedlejší ústřednu;

b) *vícestupňové EPS* – mají hlavní a vedlejší ústředny, na které jsou připojeny samočinné a tlačítkové hlásiče požáru a vedlejší ústředny nižšího stupně;

c) *EPS s kolektivní adresací* – v současné době jsou používány dva systémy EPS; u systému EPS s kolektivní adresací je sice ústředna schopna rozlišit z které hlásicí linky přišel signál POŽÁR, ale nezjistí, od kterého konkrétního hlásiče; tento systém není optimální, neboť neumožňuje přesně určit místo požáru, čímž může dojít k prodloužení doby pro včasný a efektivní zásah;

d) *EPS s individuální adresací* – tento systém umožňuje identifikaci stavu jednotlivých hlásičů na hlásicí lince.

Součásti systému EPS

Systém EPS se skládá se z ústředny EPS, tlačítkových a samočinných hlásičů požárního poplachového zařízení, požárních kabelů, adaptérů a dalšího příslušenství.

Ústředna EPS

Ústředna EPS je zařízení, které přijímá a vyhodnocuje výstupní elektrické signály hlásičů, signalizuje a vysílá informace o vlastním provozním stavu, ovládá doplňující zařízení EPS a přímo či nepřímo ovládá zařízení bránící rozšíření požáru, popř. zařízení provádějící samočinně protipožární zásah. Mezi další funkce ústředen EPS patří i návaznost na centrální ozvučovací systém budovy, klimatizaci, požární odvětrávání, výtahy, únikové východy apod.

Hlásiče požáru

Hlásiče požáru jsou zařízení, které reakcí na daný signál vytváří výstupní elektrický signál, a to buď samočinně, nebo jsou uvedeny do činnosti osobou. Dělíme je na:

a) *tlačítkové hlásiče* – při promáčknutí čelního skla se sepne spínač; tlačítkové hlásiče umísťujeme tam, kde je stálá přítomnost personálu; sklo na hlásičích je možno nahradit plastovou (nerozbitnou) fólií;

b) *samočinné hlásiče* – na základě změn sledovaných fyzikálních veličin se samočinně uvedou do poplachového stavu; tyto hlásiče reagují buďto na přítomnost teploty nebo kouře;

c) *ionizační hlásiče kouře* – princip detekce je založen na měření vodivosti v ionizační komoře, diference mezi vodivostí měřicí a referenční komory; po překročení určité statické hodnoty se hlásič přepne do poplachového módu; tyto hlásiče přestávají být v současné době v Evropě z ekologických důvodů používány;

d) *opticko-kouřové hlásiče* – ke své činnosti využívají pulzující LED diodu umístěnou uvnitř hlásiče; po proniknutí kouře do komory způsobí částice kouře rozptyl světla a hlásič se přepne do poplachového módu.

e) *hlásiče teplot* – ke své činnosti využívají vnitřní a vnější termistory; pokud jejich nerovnováha překročí určitou mez, dojde k vyhlášení poplachu; v případě, že teplota vzrůstá pomaleji, zareaguje hlásič na překročení stanovené teploty; tímto optimálním uspořádáním zajišťuje hlásič včasnější hlášení poplachu.

Speciální hlásiče

lineární hlásiče tepla – lineární systém hlášení tepla pro rozpoznání požáru a přehřátí, např. v kabelových kanálech, nádržích s plovoucí střechou

v petrochemii, parkovacích garážích, kompostovacích zařízeních, pásových dopravnících a skládkách odpadu,

- *lineární optické hlásiče* – detekce kouře na základě principu světelné závory pro montáž na protilehlé stěny,
- *systémy nasávání kouře* – systém nasávání kouře z uzavřeného prostoru pomocí sítě potrubí,
- *hlásiče pro vzduchotechniku* – pro detekci kouře ve vzduchotechnických kanálech,
- *hlásiče detekce CO* – slouží k upozornění při vzniku prudce jedovatého oxidu uhelnatého označovaného jako CO plyn.

Přídavná zařízení EPS

Jedním z přídavných zařízení EPS je zařízení dálkového přenosu. Umožňuje přenos alespoň základních provozních stavů POŽÁR a PORUCHA na určené místo, nejčastěji na ohlašovnu požárů. Přenos je zajištěn i v nepřítomnosti, či selhání obsluhy. Pro usnadnění obsluhy ústředny EPS jednotkou PO v případě požáru signalizovaného EPS se připojují tzv. obslužná pole požární ochrany (OPPO), jejichž prostřednictvím je možno provádět základní obsluhu EPS. Pro usnadnění vstupu jednotky PO do objektu je možno použít klíčový trezor požární ochrany (KTPO), který je ihned po potvrzení poplachu z ohlašovny požáru automaticky odblokován z ústředny PZTS. Zařízení pro odvod kouře a tepla (ZOKT) je zařízení umožňující automaticky nebo ručně (pomocí tlačítka) otevřít střešní okno, které plní funkci kouřové klapky a odvést tak mimo prostory kouř, plyny a teplo vznikající při požáru. Systémy požárního větrání jsou napojeny na ústřednu EPS. Jejich činnost nesmí ovlivnit funkci sprinklerových hlavic a detektorů kouře. Protipožární únikové dveře jsou vyráběny ze speciálních dveřních profilů s utěsněním proti prachu, hluku a úniku tepla. Dveře jsou napojeny na EPS a při požáru se samy otevřou.

Použitá literatura

ČSN 34 2710 Elektrická požární signalizace – Projektování, montáž, užívání, provoz, kontrola, servis a údržba. Vydal ÚNMZ, zpracovatel: AGA, Centrum technické normalizace pro bezpečnostní služby, ve spolupráci s Cechem EPS ČR, ve spolupráci s pracovním kolektivem ve složení (řazeno abecedně): Miroslav Budín, Ing. Milan Holas, plk. Ing. Zdeněk Hošek, Ing. Jan Jiskra, Jiří Juhaňák, František Krejčí, Ing. Jiří Laifr, Václav Levíček, Martin Motyčka, TNK 124 EPS a poplachové systémy, pracovník ÚNMZ Ing. Radek Špaček. Září 2011.

6.3 Dohledové a poplachové přijímací centrum (DPPC)

Ivo Popardowski

V důsledku neustále rostoucí kriminality vyvstává obecně stále větší potřeba chránit své zdraví, život i majetek lidí. Tato nutnost vedla již v minulosti k vývoji a instalování takových bezpečnostních zařízení, která by umožnila včasné hlášení poplachových (havarijních) situací ze vzdálených objektů do centrálního dispečinku pro střežení. Ovšem i použití nejkvalitnějších mechanických, technických a elektrických zábran se často míjelo účinkem, dokud samotná jejich funkce nebyla posílena o efekt zajištění účinného zásahu lidským faktorem. Zařízení sloužící k tomuto účelu, dříve známá jako pulty centrální ochrany (PCO), jsou dnes označována jako dohledová a poplachová přijímací centra (DPPC).

K výše zmíněnému účelu začala postupně vznikat zařízení, která jsou dodnes obecně nazývaná pulty centrální (později centralizované) ochrany. V zemích dřívějšího tzv. východního bloku začal vyrábět pulty centrální ochrany pod názvem NĚVA (tehdejší Sovětský svaz). V rámci Rady vzájemné hospodářské pomoci (RVHP) dostalo následně souhlas k výrobě také Bulharsko, které na trh uvedlo obdobné zařízení pod názvem RONA. K nám se tyto výrobky dovážely ve větším měřítku v letech 1974–1976. Jako historicky první začal PCO používat v tehdejší ČSSR útvar Služby ochrany majetku Veřejné bezpečnosti (VB). Jeho úkolem bylo zajišťovat vlastními silami střežení strategicky významných státních institucí a objektů, bank, čerpacích stanic, kulturních objektů a větších poštovních poboček. K přenosu signálu (zpráv) mohl využívat výhradně telefonní linky v základním hovorovém pásmu. Střežené objekty byly propojeny s městskou telefonní ústřednou a přes tzv. výkonový díl napojeny na „policejní" PCO. Vlastní zapínání střežení objektu taktéž fyzicky prováděli na svých stanovištích příslušníci VB, ovšem pouze mimo provozní dobu objektu. Zastřežením objektu se totiž přerušila možnost dalšího využívání telefonní linky, zejména běžného telefonování. Tehdejší pulty se skládaly pouze ze spínačů a kontrolních žárovek (později LED), jež signalizovaly stav zastřežení objektu. Neumožňovaly žádné další dělení na podskupiny nebo zóny, technicky možná nebyla jakákoliv archivace přijatých zpráv.

Ještě v roce 1989 střežili tímto způsobem pracovníci Služby ochrany objektů VB téměř osm tisíc objektů. Větší pokrok zaznamenalo teprve vyřešení možnosti přenosu zpráv v tzv. nadhovorovém kmitočtovém pásmu 20 kHz koncem osmdesátých let. V Československu byl vyvinut nadhovorový pult

GENOVA, který byl veřejnosti představen v roce 1991 na první porevoluční výstavě bezpečnostních technologií InterAlarm (dnešní veletrh PRAGOA LARM). S masivnějším využíváním počítačů se začaly postupně vyvíjet také různé aplikace, které zajišťovaly kódový překlad, zobrazení a základní archivaci dat.

Po roce 1989 se pulty centrální ochrany rozšířily také do oblasti zájmu komerční bezpečnosti, a to především v důsledku zvýšené poptávky na střežení nestátních komerčních objektů. Díky rychlému vývoji a rostoucí konkurenci výrobců se záhy začala objevovat zařízení, pracující na principu rádiového přenosu. Nedílnou součástí PCO se staly tzv. zásahové jednotky, které se dokázaly dostat v relativně krátkém čase na ohrožené místo, a mohly tak s daleko větší pravděpodobností zadržet pachatele, popřípadě dočasně zajistit napadený objekt.

Dohledové a poplachové přijímací centrum (DPPC).
Foto Tomáš Popardowski. Zdroj: ABAS IPS Management.

Terminologie

S masivní expanzí moderních a cenově dostupných zabezpečovacích systémů a technologií vyvstala potřeba zajistit, aby si mezi sebou porozuměli nejenom jejich provozovatelé a uživatelé, ale také projektanti, zástupci výrobních podniků, dovozci pracovníci montážních a servisních středisek, investoři a v neposlední řadě zákazníci. To znamenalo sjednotit základní terminologii. Účelem jednotné terminologie je dopomoci k tomu, aby například zkratka EPS nebyla jednou chápána a vysvětlována jako „elektrický požární systém", podruhé jako „elektronický požární systém, potřetí jako „elektronická požární signalizace atp. Nehledě k tomu, že většina kompo-

nentů poplachových zabezpečovacích systémů (PZS) a elektrické požární signalizace (EPS) patřila a dodnes patří do skupiny výrobků v kategorii „elektrická", nikoli „elektronická" zařízení. Navíc jsou regulována směrnicemi EU, případně dalšími legislativními nařízeními, jež stanovují technické požadavky na výrobky regulované sféry pro možnost jejich zavádění na unijní trh. Jen pro zajímavost – k výrobkům regulované sféry patří například hračky, výtahy, stroje, tlakové nádoby, plynové spotřebiče, zdravotnické pomůcky, výměníky tepla, stavební prvky, zbraně a výbušniny, osobní ochranné pomůcky, potraviny a další.

Pomineme-li nejstarší terminologii, používal se pro poplachové systémy do roku 2002 jednotný název EZS – elektrická zabezpečovací signalizace. Poté byla přijata nová definice EZS, která následujících sedm roků platila ve znění elektrické zabezpečovací systémy. Aby toho ovšem nebylo málo, od září 2009 rozlišujeme dvě aktuálně platná odvětví. K prvním patří poplachový systém pro detekci vniknutí (IAS – Intruder Alarm System), pro jehož obecné pojetí se v odborných kruzích ustálil pojem poplachový zabezpečovací systém (PZS). Druhým odvětvím je poplachový systém pro detekci přepadení (HAS – Hold-up Alarm System), který je vnímán jako poplachový tísňový systém (PTS). V celkovém pojetí oboru pak nově hovoříme o I&HAS (Intruder and Holdup Alarm System), tedy o poplachovém zabezpečovacím a tísňovém systému (PZTS).

Legislativa

Protože každý návrh, realizace a provoz bezpečnostní technologie musí respektovat platné normy, byly donedávna všeobecné požadavky pro poplachové zabezpečovací a tísňové systémy upraveny normou ČSN EN 50131-1. Vlastní přenos signálů a základní zásady provozu PCO pak byly řešeny normami řady ČSN EN 50136, zejména technickými normami ČSN EN 50136-2-2 a ČSN EN 50136-1-4. Na poplachové zabezpečovací systémy se dále vztahují některé další technické normy z hlediska požadavků na elektromagnetickou kompatibilitu, elektrickou bezpečnost a telekomunikační a rádiové zařízení. V současné době, respektive s platností od 1. ledna 2011, jsou dohledová a poplachová přijímací centra řešena normami ČSN EN 50518-1, ČSN EN 50518-2 a ČSN EN 50518-3.

Normativní zásady provozu

Norma ČSN EN 50518-1 se vztahuje na veškerá dohledová a poplachová přijímací centra (MARC, ARC[3]). Stanovuje minimální požadavky na návrh konstrukci a funkční zařízení pro budovy, v nichž se uskutečňuje monitorování, příjem a zpracování (poplachových) signálů generovaných poplachovými systémy jako integrální část celkového procesu zajištění bezpečí a zabezpečení. Dohledové centrum tak musí například splňovat předepsanou sílu zdí, musí mít okna s balistickou a požární odolností, detekční zařízení plynu, dostatečné množství bezpečných datových úložišť, komunikačních tras a hardwaru, jakož i automatizovanou zálohu napájecích okruhů pro případ velkoplošného výpadku elektrického proudu. Požadavky normy se vztahují jak na případy dálkové konfigurace, v nichž více systémů přenáší informace do jednoho či více poplachových přijímacích center (ARC), tak na případy jediného centra určeného pro monitorování a zpracování poplachů generovaných jedním nebo více poplachovými systémy, nalézajícími se v tomtéž perimetru příslušného místa. Dále jsou v ní uvedeny stavební požadavky na dohledová centra z hlediska odolnosti proti napadení, proti požáru a na ohodnocení rizik. Norma ČSN EN 50518-2 se vztahuje na veškerá dohledová a poplachová přijímací centra (DPPC), která monitorují, přijímají anebo zpracovávají signály, jež vyžadují okamžitou reakci. Norma stanovuje technické požadavky, zahrnuje funkční kritéria a ověřování výkonnosti. Norma ČSN EN 50518-3 stanovuje požadavky na personál, pracovní postupy a provoz dohledových poplachových center (pultů centralizované ochrany). Dále specifikuje požadavky na výcvik, bezpečnostní prověření a lustraci personálu, v neposlední řadě pak požadavky na testování center, správu databází a likvidaci údajů, řízení nouzových stavů, evakuačních postupů a audit poplachových dohledových center.

Přenosové cesty

Stále náročnější požadavky na bezpečnější a rychlejší přenos signálu v přenosové síti jsou přímo úměrné zvyšujícímu se objemu a důležitosti přenesených zpráv. Normy přesně stanoví počty kontrol u jednotlivých stupňů zabezpe-

[3] **Redakční poznámka**: Ve všech existujících dokumentech normativní řady 50131-1, zpracovaných odborníky Evropské komise pro normalizaci v elektrotechnice CETELEM v souboru CLC/TC 79 – Poplachové systémy se používá zkratka ARC. Pro dosažení konzistence v terminologii a také proto, aby nedocházelo k nedorozuměním, je v těchto normách používána zkratka ARC, přičemž zkratka MARC je zkratce ARC ekvivalentní.

ení. Samozřejmě specifikují i mnoho dalších povinností směrem k odborně způsobilému provozovateli komunikačních přenosových tras, a to včetně případů, kdy je na základě vyššího stupně ohrožení nařízena povinnost náhradní předepsané trasy. K nejvyužívanějším komunikačním přenosovým trasám dnes patří telefonní linka ISDN, rádiový přenos na vyhrazených frekvencích, přenos po síti GSM v hovorovém pásmu, přenos po síti GSM prostřednictvím GPRS, přenos po síti GSM prostřednictvím SMS, přenos pomocí internetové sítě a přenos pomocí vyhrazených přenosových cest. U objektů s nejvyšším stupněm ohrožení (bankovních domů, strategicky významných objektů apod.) je využívána kombinace dvou přenosových cest.

Pulty centralizované ochrany poskytují v současné době mnohem rozsáhlejší služby, než je pouhé střežení objektů. Na PPC (PCO) přicházejí nejenom poplachové zprávy, ale jsou zde shromažďovány nejrůznější údaje o technologických zařízeních budov, např. o teplotách, stavu výměníkových stanic, poruchách kotelen, výtahů, klimatizací apod. Proto budeme postupem času všichni hovořit spíše o dohledovém a poplachovém přijímacím centru (DPPC).

Použitá literatura

[1] DRGA, Rudolf; ŠMIRAUS, Michal: *Dohledová a poplachová přijímací centra a jejich další vývoj*. In: LUKÁŠ, Luděk a kol. *Bezpečnostní technologie, systémy a management*. Radim Bačuvčík – VeRBum. Zlín 2011. Str. 139–147. ISBN 978-80-87500-05-7.

[2] LUČAN, Jiří: *Tvorba edukačního materiálu s prvky e-learningu systému PCO GLOBAL*. Bakalářská práce. Fakulta aplikované informatiky UTB ve Zlíně. Zlín 2007.

[3] ČSN EN 50518-1. Dohledová a poplachová přijímací centra – Část 1: Umístění a konstrukční požadavky. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. Praha 2011.

[4] ČSN EN 50518-2. Dohledová a poplachová přijímací centra – Část 2: Technické požadavky. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. Praha 2011.

[5] ČSN EN 50518-3. Dohledová a poplachová přijímací centra – Část 3: Pracovní postupy a požadavky na provoz. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. Praha 2012.

[6] ČSN EN 50136-1. Poplachové systémy – Poplachové přenosové systémy a zařízení – Část 1: Obecné požadavky na poplachové přenosové systémy. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. Praha 2012.

6.4 Multifunkční dohledové centrum (MDC)

Jaromír Kyncl (podle Pavla Kocábka a Tomáše Koníčka)

Současným trendem, který začal být uplatňován v zemích EU, je vytváření tzv. multifunkčních dohledových center. Multifunkční dohledová centra jsou budována za účelem nepřetržitého sledování a okamžité reakce na události, a to nejen systémů CCTV, ale i u ostatních zabezpečovacích systémů, požárně bezpečnostních technologií, systémů vytápění, klimatizací objektů, komunikátorů výtahových zařízení apod. Podstatně tak rozšiřují efektivitu střežení objektu a na incidenty či podezřelá jednání dokáží reagovat okamžitě a včas jim předcházet. V MDC se sbíhají veškeré měřená a zaznamenávaná data a obrazy a jsou přehledně zobrazeny na velkoplošných monitorech. MCD bývají často napojena na městskou policii, případně Policii ČR a na HZS. Pracovníci ostrahy tak mají k dispozici všechny obrazy kamer, údaje o aktuálním stavu zabezpečení objektů, požární signalizace a mohou vše pohodlně ovládat a sledovat z jednoho místa. Multifunkční dohledová centra jsou nejvyšším stupněm dosavadních pultů centralizované ochrany (PCO). Jsou vybavena špičkovými technologiemi a obsluhována zkušenými pracovníky na vysoké odborné úrovni. Mimořádná pozornost je věnována jejich spolehlivosti. Svým propojením na integrovaný záchranný systém (IZS), jsou neocenitelnými pomocníky krizových štábů a součástí jejich krizových plánů.

Zajišťování provozuschopnosti, ochrany majetku a zdraví a životů osob, požární ochrany, ochrany před ekologickými haváriemi prostřednictvím multifunkčních dohledových center představuje v současné době nejvyšší možnou známou úroveň v této oblasti. Souběžně s tím roste logicky také úroveň technického zajištění objektů, rozvíjejí se výrobní technologie, použité stavebně konstrukční prvky atd. Výhody multifunkčních dohledových center se dají velmi dobře skloubit s nejmodernějšími prvky „inteligentních" budov.

Multifunkční dohledová centra jsou zároveň ideálním místem pro zřízení centrálních propojovacích uzlů a nahrávacích center, kdy jsou v technologických místnostech osazeny rozvaděče vysokokapacitními diskovými poli pro záznam všech veličin a obrazů kamer v požadované kvalitě a délce.[4]

Popis činnosti multifunkčního dohledového centra

Multifunkční dohledové centrum (MDC) vzniklo využitím zkušeností

[4] http://www.interconnect.cz/kamerove-systemy/dohledova-centra

spojených s provozováním klasického PCO a implementací těchto poznatků do nejnovějších technologií s aplikací zakázkového softwaru. Vysoká pozornost je věnována ochraně informací. Celé pracoviště MDC má vlastní záložní systém pro dodávku elektrické energie.

Pracoviště MDC je schopno monitorovat bezpečnostní situaci a servisní potřeby stejně jako technologické i logistické procesy, kontrolovat, řídit a koordinovat činnosti související s bezpečností na jednotlivých objektech, jakož i celku jako takovém. Veškeré přicházející informace jsou svedeny do dohledového centra všemi druhy komunikačních tras, které jsou vždy dvoj až trojnásobně zálohovány. Jedná se zejména o informace hlasové a datové, hlášeny jsou stavy technologických zařízení, bezpečnostních systémů a v neposlední řadě i informace o stavu a pohybu vozidel nebo jiných mobilních objektů, lze sledovat i pohyb osob. Veškerá propojení jsou realizována na úrovni přímé integrace do infrastruktury poskytovatelů, ať již telekomunikačních nebo jiných služeb. Řešení komunikace umožňuje ten nejbezpečnější přístup k informacím zejména vlastním servisním pracovníkům, kteří tak mají kdekoli v terénu všechny potřebné informace okamžitě k dispozici. Zákazníci mají neustálý přehled o stavu na jednotlivých objektech prostřednictvím SMS zpráv, které dostávají přímo na své mobilní telefony v reálném čase prostřednictvím bezpečného přenosu. Totéž platí o jednoduché komunikaci klientů s dohledovým centrem prostřednictvím tzv. jednotného čísla, díky kterému se dovolají vždy a z každého místa v republice za cenu místního poplatku přímo na operátora, který má k dispozici veškeré potřebné informace a je schopen zajistit jakoukoli smluvní službu. Samozřejmá je možnost předávání textových a obrazových informací prostřednictvím IT sítě.

Vlastní pracoviště má svoji identickou kopii, která je umístěna geograficky jinde a vytváří jednak zálohové pracoviště, ale i možnost posílit v reálném čase vlastní dohledové centrum. Díky záložnímu pracovišti jsou všechny informace replikované na dalším hardwaru, ze kterého se teprve vytvářejí vlastní datové zálohy. Všechna tato opatření mají dostupnost poskytovaných služeb téměř 99 %.

Činnost MDC zahrnuje zejména:[5]

- vlastní napojení různých bezpečnostních systémů na multifunkční dohledové centrum všemi dostupnými prostředky,

[5] Zdroj: http://www.stavebnictvi3000.cz/clanky/multifunkcni-dohledova-centra/

- přímé spojení a úzká spolupráce s IZS,
- nepřetržitý bezpečnostní monitoring objektů zahrnující napadení, požár, signály tísní, signály ze stanovišť místní ostrahy atd.,
- bezpečnostní a logistický monitoring vozidel,
- vyrozumění oprávněných osob o poplachu v napojeném objektu,
- monitorování pohybu osob,
- výjezd a zásah stálé výjezdové skupiny po celé ČR,
- zadržení pachatele, který se nachází v napadeném objektu a jeho předání Policii ČR,
- reakci a součinnost při řešení mimořádných událostí v celé ČR,
- přenos technických a provozních zpráv (výpadky elektrického proudu apod.),
- dálkový dohled a servis napojených systémů,
- kontrolu přenosové cesty dle výběru uživatele, možnost zdvojení přenosových tras dle požadavků pojišťoven a norem ČSN EN,
- technickou pomoc uživatelům,
- možnost sledování určených časů uzamčení (zakódování) systému,
- dálkovou kontrolu překročení technických stavů (teploty, zaplavení, únik plynů, vlhkosti apod.) se zajištěním adekvátní reakce,
- monitoring a zajištění výjezdu v případech havárie plynu, vody, v krizových situacích (povodeň, požár),
- zajištění datových sítí,
- střežení objektu do příjezdu odpovědné osoby nebo policie,
- služby spojené s požární ochranou a prevencí,
- provádění plánovaných a termínovaných kontrol objektu,
- dovoz odpovědných osob,
- klíčovou službu na objektech,
- poskytnutí pravidelného či jednorázového výpisu událostí, jednotného systému pro vyúčtování (pro více objektů),

- zajištění informační bezpečnosti dle normy ČSN ISO/IEC 17799, Soubor postupů pro řízení informační bezpečnosti,
- zpracování zprávy v případě napadení objektu,
- spojení na oficiální linky pomoci,
- poradenství,
- help line 24 hodin denně.

Výhody multifunkčních dohledových center se dají velmi dobře skloubit s nejmodernějšími prvky inteligentních budov a mohou tak jednoznačně přispívat k dokonalému využití techniky a lidského potenciálu k ochraně osob a majetku, tedy k bezpečným lokalitám v různých obcích či částech větších měst.

Důležitými předpoklady pro kvalifikované provozování MDC jsou nutné minimálně následující certifikáty: certifikát České asociace pojišťoven, certifikát ČSN EN ISO 9001:2001 pro systém managementu kvality, certifikát ČSN EN ISO 14001:2005 pro systém enviromentálního managementu a certifikát ČSN BS 7799-2:2004 pro systém managementu bezpečnosti informací.

Použitá literatura

KOCÁBEK, Pavel; KONÍČEK, Tomáš: *Multifunkční dohledová centra*. In: Stavebnictví a interiér, rubrika Zabezpečovací systémy budov a objektů. Čís. 7. Portál www.stavebnictvi3000.cz, 2006.

6.5 Kamerový systém (CCTV)

Jaromír Kyncl

Trendem dnešních systémů CCTV je nejen vysoká kvalita snímaného obrazu a zvukového záznamu, ale také efektivnost a jeho jednoduchá obsluha. Získávání okamžitého přehledu o aktuální situaci i na několika od sebe vzdálených místech je pro rychlé a správné analyzování bezpečnostní situace nezbytné a nenahraditelné. Proto patří kamerový systém CCTV k nejrychleji se rozvíjejícím a také velmi často žádaným systémům. Uvažujeme-li o kamerovém systému CCTV jako o nástroji určeném pro bezpečnostní aplikace, je nutné alespoň ve zkratce popsat ty aplikace, které určuje norma ČSN EN 50132-1 – Poplachové systémy – CCTV sledovací systémy pro použití v bezpečnostních aplikacích – Část 1: Systémové požadavky. Tato norma určuje obecné požadavky na přenos videosignálu, tedy jeho výkonu, zabezpečení a shody se základním IP spojením. Dále definuje tzv. funkční bloky kamerového systému a popisuje poplachový sledovací kamerový systém jako skladbu zařízení obsahující analogové nebo digitální prvky včetně softwaru.[6]

IR digitální kamery. Foto Jaromír Kyncl.

Kamerové systémy lze používat samostatně pro monitorování obchodů, bank, veřejných prostranství či společných prostor obytných domů. Lze je také integrovat s dalšími systémy do vyšších komplexních celků. Podle konkrétních požadavků zákazníka firmy projektují a instalují CCTV společně se systémem PZTS, s identifikačními a docházkovými systémy, s perimetrickým zabezpečením a dalšími bezpečnostními technologiemi. Současné přenosové možnosti

[6] RANDA, Michal: *Guideline IP CCTV*. In: ALARM FOCUS. Čís. 2. ORSEC, s. r. o. Brandýs nad Labem 2013. ISSN 1805-9007. Str. 24–25.

komunikačních sítí totiž umožňují sdružení výše uvedených systémů do jednoho řídicího monitorovacího (dohledového, dispečerského) pracoviště.

IP kamerový systém

S technickým pokrokem zejména v oblasti přenosových sítí a v oblasti digitalizace videosignálu se začínají stále více prosazovat tzv. IP kamery (IP Internet Protocol). V pouzdře IP kamery je kromě standardní analogové videokamery instalován též integrovaný webový server, který zajišťuje digitalizaci a komprimaci videosignálu a připojení videokamery k počítačové síti.

IP kamery mají implementované webové stránky (HTTP), které umožňují sledovat obraz v libovolném internetovém prohlížeči v rámci lokální počítačové sítě stejně jako on-line prakticky z libovolného místa na světě. IP kamery jsou proto mimo jiné využívány pro zabezpečení a videomonitoring vzdálených objektů.

Celá řada vnitřních i venkovních pevných a otočných IP kamer s vysokým rozlišením zajišťuje nejvyšší kvalitu obrazu s minimálními nároky na šířku pásma v síti a na kapacitu uložiště dat. Necentralizovaná architektura umožňuje stavět systémy modulárně – od jedné kamery a jednoho rekordéru až po náročné bezpečnostní aplikace pro město, stát nebo dokonce i kontinent (s počty propojených kamer v řádu tisíců).

Analýza obrazu

Většina moderních IP kamerových systémů poskytuje uživatelům sofistikovaný systém nástroj pro analýzu obrazu, který umožňuje zlepšení pracovních výkonů operátorů CCTV a zvýšení produktivity práce při stejném nebo i nižším počtu pracovníků. K nejběžnějším využívaným typům analýzy obrazu patří funkce:

- virtuální hranice (chrání perimetr, volné příjezdové cesty),
- detekce pohybu ve špatném směru (upozorní na pohyb v nepovoleném směru),
- detekce krádeže (sleduje přítomnost pouze statických předmětů, ignoruje pohyb),
- detekce zakrytí kamery (chrání kameru před sabotáží, např. přestříkání sprejem),
- detekce zanechaného předmětu (plní antiteroristickou funkci),

- detekce zaplnění prostoru (upozorňuje na zaplnění oblasti zájmu, plní zadání pro statistické účely),
- počítadlo průchodů, průjezdů aj.

V systémech CCTV se také stále častěji setkáváme s termovizními kamerami, u nichž lze lépe využít některých prvků videoanalýzy díky téměř neměnné podobě obrazu za všech světelných a povětrnostních podmínek. V oblasti tzv. objemové detekce s možností sledování pohybu objektu se stále častěji objevují pozemní FM-CW radary využívající dopplerovského efektu, které byly ještě donedávna výsadou pouze armádních složek.[7]

K dispozici je také široký výběr kamer se speciálně upravenými kryty pro sledování například výrobních procesů, u nichž je přítomnost a kontrola obsluhy nemožná z důvodů vysoké teploty, chemicky agresivního, nebo dokonce výbušného prostředí apod.

6.6 Řízené docházkové a přístupové systémy (AKV, ACS)

Milan Říha, Ladislav Sieger, Pavel Pikola

Požadavky na vstupní dveře

Při první instalaci systému kontroly přístupu je třeba si ujasnit odpovědi na otázky týkající se jednotlivých vstupních bodů a prostupů:

a) Mají se dveře otevírat vždy jen při kontrole vstupu nebo mají zůstat otevřené během určité doby, např. pracovní doby?

b) Má být možné, aby za určitých podmínek otevřela osoba dveře jen zmáčknutím tlačítka a má být k tomu účelu instalováno dorozumívací zařízení nebo videointerkom?

c) Smí být za určitých podmínek dveře otevřeny někým jiným než pracovníkem kontroly přístupu, např. ohnivzdorné dveře v případě požáru?

d) Musejí být dveře po skončení práce uzamčeny v souladu s požadavky pojišťovny?

e) Nacházejí se dveře v únikové cestě (jestliže ano, pak musí po technické stránce splňovat požadavky příslušných předpisů)?

[7] ZACHOVAL, Radek: *Současné trendy v systémech CCTV*. In: Security magazín. Čís. září/říjen 2012. Security Media, spol. s r.o. Praha 2012. Str. 17.

f) Jedná se o dveře normální, turniket či dveře stahovací?

g) Mohou dveřmi procházet i osoby tělesně postižené (toto může mít vliv na výšku instalace čtečky, do níž se vkládá karta)?

h) Je průchod normálně nebo mimořádně široký (např. aby bylo možno projet vozíkem s materiálem)?

i) Jsou dveře vně objektu a mohou být ohroženy vandalismem (pak je třeba dát přednost bezdotykovému zařízení)?

Dveře v regulačním obvodu

Zábranný systém kontroly přístupu je mechanické nebo elektromechanické zařízení, které při pozitivním rozhodnutí o oprávněnosti přístupu uvolní vstup, rozezná stav odemčení či uzamčení a dá zpětné hlášení ústředně kontroly přístupu. Zábranným zařízením kontroly přístupu jsou zámky, turnikety, elektrické branky nebo závory. Senzory zpětného hlášení jsou kontakty, vypínače a tlačítka.

K detekci otevření nebo průchodu dveří slouží různé typy detektorů (magnetické kontakty, infrazávora apod.). Na základě jejich aktivace se zjistí, zda po uvolnění dveří skutečně do místnosti vstoupila nějaká osoba.

Únikové cesty

Možnost uniknout musí mít naopak všechny přítomné osoby v případě mimořádné události, např. požáru. Únikové východy slouží k rychlé evakuaci osob z objektu. Při plánování systému kontroly přístupu nelze zapomínat na únikové cesty.

Prvky kontroly přístupu

Mezi funkce systému kontroly přístupu patří také ochrana před neoprávněnou manipulací (použitím neplatného vstupníku, zkoušením různých kódů) a signalizace otevření dveří nad povolený časový limit. Jsou však prvky kontroly přístupu a okolí bezpečné? Terminál je střežen před pokusy otevřít dveře. Také existuje kontrola vůči vypáčení dveří a je možná i signalizace pokusů o manipulaci na vedení k otvírači dveří. Jinak je tomu ale při manipulaci se čtečkou. Čtečka magnetických karet, ať se již jedná o zařízení vsunovací, vtahovací či protahovací, může být vždy snadno učiněna nefunkční pomocí papíru, žvýkačky nebo tekutin. To však není u čteček bezkontaktních. Bez-

kontaktní čtečka může být přídavně zajištěna tím, že ji v prostoru, který má být chráněn, namontujeme tak, že vstupníky mohou být přečteny na delší vzdálenost (např. 25 cm) i přes zdivo budovy. I při zničení vnějšího zdiva zůstanou dveře uzamčeny, neboť vlastní čtečka je ukryta na vnitřní straně zdi.

Oprávněná osoba a druhy oprávnění

Oprávněná osoba je taková osoba, která má oprávnění být na určitém místě v určitý čas. Oprávněnými osobami nejsou jen vlastní zaměstnanci, nýbrž i návštěvníci (zákazníci, dodavatelé, obchodní zástupci apod.), a také externí pracovníci (opraváři, uklízečky apod.). Návštěvníci a externí pracovníci jsou však jen částečně oprávněnými, neboť mohou vstupovat jen v určitou dobu do určitých prostorů. Také vlastní zaměstnanci mohou mít omezen přístup do určitých prostorů v určitou dobu (např. do místnosti s počítači, do pokladny apod.).

Druhy oprávnění

Vstupní oprávnění se vztahují na prostorové anebo časové zóny, přičemž konkrétní osoba může mít více druhů oprávnění, například:

1) generální oprávnění ke vstupu – vstup do všech prostorů a v každé době,
2) omezené generální oprávnění ke vstupu – vstup do všech prostorů a v každé době, ale jen pod dohledem (např. personál úklidu),
3) časově omezené oprávnění ke vstupu – vstup do všech prostorů, ale jen v určité době,
4) prostorově omezené oprávnění ke vstupu – vstup do jednoho nebo více prostorů v každou dobu,
5) prostorově a časově omezené oprávnění ke vstupu – vstup do určitých prostor pouze v určité době (např. vstup do osobního oddělení jen mezi 9. a 11. hodinou apod.),
6) oprávnění vstupu s omezeními,

a) vstup jen tehdy, je-li v prostoru nikoli více než X osob,

b) vstup jen tehdy, je-li v prostoru současně nejméně X osob;

c) vstup jen společně s osobou XY,

d) není přístup do prostoru A, byla-li osoba před tím v prostoru B,

e) není přístup do prostoru B během určitého časového úseku.

Z hlediska různých druhů oprávnění se tedy systémy kontroly přístupu rozlišují podle druhů zón:

a) jednoduché systémy otevírání – při pozitivní identifikaci se dveře otevřou,

b) poplachové systémy – je-li kód chybný, spustí se poplach (možnost 3x zadat špatně PIN, pak poplach),

c) identifikační systémy registrující přítomnost osob v objektu.

Kontrola

Kontrolou se rozumí všechny mechanismy, které po prověření oprávněnosti vstup povolí či nikoli. Jak dlouho se musí na otevření dveří čekat, závisí na mnoha faktorech. Jako první faktor lze uvést to, jak rychle dotyčná osoba vloží kódovou kartu, zadá kód na klávesnici, jak pracuje čtečka, jak rychle a správně je položen prst pro biometrickou identifikaci nebo obličej do kamery. Druhým faktorem je přenos a zpracování dat a jejich verifikace (např. vyhledání uloženého referenčního vzoru při biometrické identifikaci).

Střežení

Střežením rozumíme jak již zmíněná omezení vstupu, např. „nikoli více než X osobám současně“ nebo „nikoliv méně než X osobám současně“, tak i zjištění počtu přítomných osob v jednotlivých prostorech z bezpečnostních důvodů.

Mezi významné aspekty střežení patří i funkce „anti-pass-back“, což je funkce zamezující přístupu více osob identifikujících se opakovaně již použitým vstupníkem (kartou). Nejlepší systémy umožňují také funkci „global anti-pass-back“, která spočívá navíc ve zohlednění většího počtu vstupních bodů a více střežených zón.

Poplachové řízení a poplachová organizace

a) regulérní poplach – správná funkce detektoru při narušení objektu,

b) falešný poplach – např. příliš citlivý PIR detektor zaznamená zvíře (např. kočku, psa),

c) záměrný poplach – vyvolaný pachatelem; zásahová jednotka se dostaví na objekt, nezjistí narušení objektu, vrací se zpět na základnu; po několikerém opakování pak obsluha PCO ústřednu deaktivuje a pachatel provede vloupání do objektu.

Přístupové vstupní terminály

Elektronický klíč

Elektronický klíč je též nazýván čipový klíč. Inteligentní uzamykací systém může sestávat z klíče s mikroprocesorem (čip-klíč), zámku a elektroniky. Tato řídicí jednotka se nachází např. v separátní schránce pod vlastním zámkem. Řídí všechny zamykací a jiné postupy, obsahuje hodiny s přesným časem a dlouhodobým kalendářem a uchovává všechna data, jež jsou důležitá pro uživatele (provozovatele). Elektronika potřebuje energii. Malé lithiové články mají elektroniku zásobovat proudem asi jeden rok. Přenos energie a výměnu dat mezi zámkem a klíčem přebírá „kombinace vysílač – přijímač" nad cylindrickou vložkou. Vybije-li se baterie, přestane elektronika fungovat a dveře lze otevřít mechanicky každým vhodným klíčem. Programování lze provádět přímo v terminálu, nebo pomocí přenosného počítače a speciálního softwaru. Tímto způsobem lze klíčům (uživatelům) přiřadit různé časové úseky a měnit oprávnění, např. zrušení při ztrátě jednoho klíče. Programovacím přístrojem mohou být též vytištěny údaje uchovávané v paměti. Vyčtená data lze rovněž převést do počítače a tam dále zpracovat. Máme-li již počítač a více než jedny dveře, mohli bychom myslet na propojení. K tomu potřebujeme síťovou kartu LAN, Ethernet aj. a příslušné rozhraní pro klávesnici s řídicí jednotkou.

Čipové karty

Původně se používaly děrné štítky, které byly později nahrazeny magnetickými pásky. Kontrola přístupu však potřebovala více informací, než mohl poskytnout děrný štítek. Proto se počaly na zadní stranu malého štítku lepit proužky magnetického pásku a tak se zrodila magnetická karta. Nevýhodou magnetické karty je její rychlé opotřebování. Z důvodu nutnosti zesílení ochrany proti zneužití a pro možnost uchování většího množství dat se začaly používat tzv. čipové karty, vybavené mikročipem s pamětí. Karty lze používat všude u peněžních automatů, u čerpacích stanic, v jídelně, u kontroly přístupu.

Čtečka a terminál

Terminál a čtečka vybavená klávesnicí, displejem, pamětí událostí a popř. další elektronikou. Čtečky rozlišujeme podle různé techniky (vsunovací, protahovací, motorové, bezkontaktní) a různého způsobu čtení (magnetický, infračervený, induktivní, bezkontaktní, handsfree, čárový kód, Wiegand, čip kartový apod.):

a) nosičem identity s integrovaným nebo naneseným magnetickým proužkem (kreditní karty),

b) u infračervené čtečky se zjistí informace uchovaná v nosiči identity optoelektronicky,

c) u induktivního postupu je informace uchována v měděné folii, která je neviditelně integrována v nosiči identity,

d) Wiegandův postup je označován jako zvláštní případ induktivního čtení, ačkoli se jedná o speciální magnetizaci nosičů identity – čipová karta obsahuje mikročip,

e) nosiči identity pro bezkontaktní (handsfree) čtení mohou vyhlížet jako čipové karty, obsahují však vysílač.

Kódová klávesnice

Použití vstupníků a čteček lze v krajních případech nahradit zadáváním PIN kódů na kódové klávesnici. Kromě toho bývají i čisté klávesnicové terminály u bezkontaktních nosičů identity a u biometrické kontroly přístupu. V prvním případě slouží klávesnice s podáním PIN jako doplňkové bezpečnostní opatření, v druhém případě pomáhá podání PIN při rychlém vyhledání příslušného referenčního vzoru. Ale i terminály s běžnou čtečkou mají často integrovanou číselnou klávesnici, většinou s doplňkovými funkčními klávesnicemi. Funkční klávesy jsou potřebné, je-li terminál používán k různým potřebám. Pro současné podchycení času existují např. funkční klávesy PŘÍCHOD, ODCHOD, SLUŽEBNĚ, LÉKAŘ apod. Pomocí funkční klávesy se lze dotázat i na stav osobního časového konta. Tento stav zobrazí displej.

Bezkontaktní přístupové systémy

Vstupník

Nosiče identity pro bezkontaktní čtení nazýváme vstupníky. Jsou nejen ve formě čipových karet, nýbrž i v podobě skleněných trubiček, přívěsků, klipsen na průkazy a náramkových hodinek. Čtecí vzdálenost mezi vstupníkem a čtečkou se různí: 5–10 cm, 20, 25, 60, 70 a 91 cm. Čím je větší plocha antény na čtečce, tím může být větší vzdálenost ke vstupníku. Druhým faktorem pro tuto vzdálenost je to, zda je identifikační systém aktivní nebo pasivní. U aktivních systémů se ve vstupnících nachází baterie. Vstupníky jsou v klidu

tak dlouho, dokud nejsou aktivovány elektromagnetickým polem určité
ho kmitočtu. Naopak pasivní systémy dostávají energii z anténového pole
dekodéru.

Čipy v nemocnicích

Ve špičkových nemocnicích jsou pacienti při příjmu vybaveni jakýmsi nára
mkem (např. HP Memory Spot), který umožňuje jejich další naprosto bez
chybnou identifikaci. Tak se nemůže stát, že si personál nemocnice splete
pacienty a těmto podá např. léky náležející někomu jinému apod. Další výho
dou čipu HP Memory Spor oproti čipům RFID je, že na něj lze ukládat text,
zvuk a krátká videa.

Kontrola vjezdu automobilů

U pasivních systémů činí vzdálenost čtení maximálně 70–90 cm. Přitom se
vstupníky nesmějí nacházet v blízkosti kovů, protože by byl silně potlače
ván výkon vysílání. Taková bezkontaktní kontrola je vhodná také pro osobní
automobily. U pasivních systémů je rozeznání více vstupníků možné jen za
zvláštních podmínek a jen v malém rozsahu. U aktivních systémů lze přečíst
současně až 30 vstupníků, což může přicházet v úvahu při identifikaci moto
rových vozidel a kontejnerů.

Volné ruce (hands free)

Vstupník může být přečten na vzdálenost cca 10 cm i přes stěnu, za níž je
instalována čtečka mimo dosah vandalů. Čtecí anténa může být skrytě in
stalována do stěny, za dřevo, plastik nebo sklo. Čtecí antény jsou odolné vůči
kondenzované vodě, dešti, sněhu a ledu. Jejich životnost je až 30 let. Pracuje
li čtečka na vzdálenost 70 cm a při přiblížení osoby otevře dveře, lze hovořit
o pravé hands free čtečce, která nenutí přicházející osobu hledat nosič iden
tity po kapsách, nýbrž mu umožní projít dveřmi třeba s plnou náručí spiso
vého materiálu.

Použitá literatura

ŘÍHA, Milan; SIEGER; Ladislav, PIKOLA, Pavel: *Bezpečnostní systémy II.* Vydání druhé ak
tualizované. Námořní akademie České republiky. Praha 2011. ISBN 978-80-87103-35-7.
Str. 148–153.

6.7 Elektronická ochrana zboží (OZ)

Jaromír Kyncl

Majitel každého objektu, do něhož má přístup více osob, zejména široká
veřejnost, se denně setkává nejenom s rostoucí kriminalitou, ale i s vynalézavostí a v mnoha případech i se stále dokonalejším technickým vybavením pachatelů. Proto musí chránit nejenom objekt jako celek, ale především své zboží
ve skladovacích prostorách, výkladních skříních, vitrínách, regálech a v nejposlední řadě též dohlížet na drobné výrobky vystavené volně na pultech.

Mobilní terminál s rozhraním RFID umožňuje snadno napsat a posléze i číst informace o specifikacích výrobku, datu výroby, údajích plomb na bázi RFID či o intervalech pro údržbu zařízení. Foto archiv Jaromíra Kyncla.

Pomineme-li nezbytné mechanické doplňky zabezpečovacích systémů pro ochranu zboží, například speciální bezpečnostní ramínka pro bezrizikové vystavení luxusních oděvů před prodejnou, plastové boxy na audio a video nosiče a SW produkty, upravené stojany a ochranné kabely pro zabezpečení fotoaparátů, kamer, mobilních telefonů, GPS navigací, patří dnes k nejfrekventovanějšímu vybavení veřejných obchodních prostor objektů některá z technologií zabývající se elektronickou ochranou zboží. Nejenom proto, že investice do ní se investorovi ve většině případů vrátí již během několika měsíců, ale také z důvodu, že mnoho výrobců je dnes schopno navrhnout a realizovat systémy elektronické ochrany zboží vhodné pro objekty všech typů, s přihlédnutím k jejich lokalitě, velikosti a také skladbě sortimentu zboží. Téměř všechny bezpečnostní technologie využívají bezkontaktní identifikační média, jsou integrovatelné do většiny kamerových systémů a jejich variabilní typologie umožňuje jejich rozšiřování a integrovatelnost do dalších bezpečnostních technologií. Tím je zajištěna optimalizace pořizovacích nákladů a dalších případných investic do budoucna.

K nejfrekventovanějším patří detekční anténní systémy radiofrekvenční (RF), elektromagnetické (EM) a akustomagnetické (AM). Většina z nás je zná spíše pod obecným názvem bezpečnostní brány. Zvláštní kapitolou jsou systémy lokálního elektronického zabezpečení, jež jsou nazývány smyčkové systémy.

Radiofrekvenční systémy

Při eliminování krádeží vykazují značnou účinnost radiofrekvenční systémy, které se používají především v obchodech se sortimentem oděvů, bot, sportovních potřeb, drogistického zboží, zařízení elektro, hraček a v hypermarketech. Radiofrekvenční systémy se skládají ze tří základních komponentů.

Prvním je detektor s jednou nebo více anténami, který vytváří ochranný prostor u východu z prodejní části.

Druhým komponentem jsou různé etikety, jež se připevňují na zboží a kterých je v současné době k dostání několik druhů. Pokud je zboží zaplaceno, etiketa se sejme (pevná) nebo deaktivuje (samolepicí). Při průchodu se zbožím s aktivní etiketou kolem detektoru je spuštěn poplach. Pevné plastové etikety jsou ke zboží upevněny hřebíčkem, tzv. pinem. Pokud zboží nelze propíchnout, připevňují se k němu plastové etikety pomocí krátkého ocelového lanka. Samolepicí etikety se používají především pro ochranu papírenského a drogistického zboží či sportovních potřeb. Dodávají se bez potisku, popřípadě také s falešným čárovým kódem. Při jejich pořizování je nutno se ujistit, zda pracují na potřebné frekvenci, obvykle 1,9 MHz, 2,4 MHz, 3,25 MHz nebo 8,2 MHz. Existují samozřejmě i etikety pracující na jiných než běžných frekvencích, například 10 MHz (papírové), které jsou dodávané zejména knihovnám.

Třetím komponentem jsou detechery pevných etiket a deaktivátory etiket samolepicích.

Při pořizování anténních detektorů je nutno brát v potaz také rozdíly mezi jedno a víceanténními systémy. Pokud je chráněn průchod cca do 2 m (při doplnění dvěma pasivními anténami až do 3,2 m) a jsou používány pouze větší a pevné (plastové) etikety, postačí jednoanténní radiofrekvenční detektor, který má samozřejmě i nižší pořizovací cenu. Je-li však součástí výstupu z bezpečnostní analýzy nutnost používat různé druhy etiket (včetně samolepicích), je vhodnější instalování víceanténního systému. V takovém případě

sice stoupnou pořizovací náklady, nespornou výhodou však bude možnost použití celého sortimentu menších etiket, dosažení většího omezení citlivosti na prostor mezi anténami a širší chráněný průchod. K základním prvkům tohoto systému je možno pořídit či nainstalovat jako příslušenství některá další zařízení, jakými jsou blokování dveří, stínění k anténním systémům, bezdrátové detektory etiket nebo napojení na vzdálený alarm.

Elektromagnetické systémy

Elektromagnetické systémy mají velmi elegantní design anténních rámů a využívají se zejména při ochraně zvukových nosičů, spotřební elektroniky a dárkových předmětů, dále v parfumériích, drogériích, obchodech s domácími potřebami, železářstvích, knihkupectvích a knihovnách. Jejich obrovskou výhodou je odolnost ochranných prvků proti odstínění alobalem. Elektromagnetické etikety lze použít na zboží kovového charakteru či na obalech s hliníkovým postřikem; jsou přitom velmi malé a nenápadné, ve formě samolepicí, vkládací či tzv. vhazovací. Elektromagnetické systémy obecně vykazují nadstandardní provozní spolehlivost, minimální nároky na údržbu a schopnost perfektní detekce ve všech třech polohách etikety v prostoru detekčních bran (tzv. 3D detekce). Vedle akustické signalizace poplachového signálu je téměř na všech anténách (branách) k dispozici rovněž světelná signalizace. V nestandardních provedeních se dá elektromagnetický systém spolehlivě využívat také při ochraně majetku a vybavení firem a jejich kanceláří (ochrana PC a příslušenství, obrazů apod.).

Akustomagnetické systémy

Akustomagnetické systémy pracují na stejném principu jako oba předchozí systémy, rovněž s možností použití jedno či víceantenních systémů. Nacházejí svoje využití zejména v místech, kde jsou velmi široké vstupy, protože dokáží spolehlivě pokrýt i přes dva metry široký prostor mezi detekčními rámy. Využívají se při ochraně konfekce, spodního prádla a dalších textilních výrobků, obuvi a kožené galanterie, potravin, alkoholických nápojů, drogistického a sportovního zboží, keramiky, skla, hraček apod. V drogeriích a parfumeriích stále častěji nahrazují elektromagnetické systémy. Akustomagnetické etikety, zejména samolepky, jsou relativně menších rozměrů a nabízejí se i v podobě vhazovacích etiket, např. do obalových krabiček s drahými parfémy.

Smyčkové systémy

Výrobci zařízení pro elektronickou ochranu zboží nezapomínají ani na ochranu výrobků vystavených volně k vyzkoušení zákazníkům. Vyvinuly se a stále se zdokonalují nejrůznější systémy tzv. smyčkové (též kabelové) ochrany, a to od nejjednodušších až po rozsáhlé inteligentní systémy, samozřejmě integrovatelné do kamerových systémů (CCTV). Kabelovou neboli „lokální" ochranou zboží proti odcizení rozumíme takovou elektronickou verzi ochrany zboží, kdy je dotyčné zboží v přímém kontaktu se zabezpečovacím zařízením, nejčastěji pomocí kabelů s kontaktními senzory nebo průvlečnými smyčkami. Výjimkou nejsou ani duální (přídavné) senzory pro ochranu odnímatelných částí zboží. Tento systém představuje nejvyšší úroveň zabezpečení ochrany zboží, prakticky stoprocentní, neboť funguje na principu uzavřeného elektrického obvodu. Jakýkoli pokus vedoucí k odstranění dotykového senzoru z chráněného zboží, přestřižení kabelu senzoru nebo jeho zkratování, vyvolá akustický alarm doprovázený blikáním LED diod na napadených senzorech, na rozvodných lištách nebo na ústředně. Ta je využívána rovněž k zabezpečení dvířek vitrín a skříněk, kdy je senzor nahrazen magnetickým kontaktem.

Mikroelektronika v boji proti krádežím

Technologie RFID (Radio Frequency Identification; radiofrekvenční identifikace) je dnes v různých formách a podobách již téměř běžnou součástí každodenního života. Jejím nejjednodušším a nejrozšířenějším využitím v praxi jsou detekční zařízení užívaná například v hypermarketech, sloužící k identifikaci zboží na principu využití systému čárových kódů nebo tzv. tagů.

V současnosti jsou RFID čipem opatřovány různé druhy zboží v prodejnách, a to buď ve formě nálepky s čárovým kódem, nebo tzv. tag nosičů informací. Při průchodu pokladním systémem jsou čipy v podobě nálepek deaktivovány a tagy, které jsou pak znovu použitelné, jsou ze zboží snímány pomocí speciálních kleští. Pokud se tak nestane, detekční rámy umístěné u východu z prodejny aktivní RFID čip zaregistrují a okamžitě spustí poplach. Dnes je však již zcela zřejmé, že využití RFID čipů rozhodně neskončí u instalace a využívání detekčních rámů k ochraně zboží proti zlodějům v prodejnách.

Ve skladech a prodejnách

U novějších typů nosičů informací začíná proces rádiové identifikace skenováním palet zboží, které opouštějí distribuční centrum. Pracovník obchodního řetězce může sledovat každou dodávku pomocí skladového informačního systému, takže ví, kdy a jaké zboží může očekávat. Jakmile jsou palety dodány do obchodu, odhalí další rádiová kontrola, zda některé bedny nechybí. Odpadá tak nutnost kontrolovat každou paletu zvlášť a osobně přepočítávat dodávky. Tímtéž způsobem začíná fungovat i logistický systém v rámci rutinního provozu v moderní obchodní síti. Čtečka RFID zabudovaná v regálech se zbožím vyšle zprávu informačnímu systému supermarketu vždy, když začne zásoba zboží na regálech docházet. Díky včasnému doplňování zboží mohou být výrazně eliminovány potenciální ztráty tržeb v důsledku vyprázdnění regálů. Každý výrobek je přitom opatřen štítkem, pomocí něhož systém sleduje, jak rychle se dané zboží prodává, a registruje nejvíce a nejméně prodávané položky. Štítky, které zároveň chrání výrobek před krádeží, jsou naposled přečteny u pokladny, kde jsou deaktivovány a na základě toho je zpětně aktualizován stav skladu. Pokud štítky u pokladny deaktivovány nejsou a zboží má prodejnu opustit, spustí senzory u východu z prodejny alarm.

Tablet PC

V nejmodernějších hypermarketech jsou na vozíky připevňovány miniaturní počítače, Tablet PC, jež identifikují zákazníka podle RFID klientské karty a na základě uloženého seznamu posledních nákupů mu doporučují zboží nové. Ke snadné orientaci v prostorách obchodu (při hledání zboží) přitom nakupujícímu slouží integrovaný navigační systém.

Smart Tags

Tenké čipy Smart Tags v sobě dokážou uchovávat a směrem k přijímacímu zařízení vysílat informace o produktu, na němž jsou umístěny. V kombinaci s pokladním systémem podporujícím tuto technologii tak výrazně urychlí a zefektivní především práci u prodejních pokladen. Ty totiž velmi rychle načtou data všech položek v nákupním vozíku a obsluha pokladny už jen vystaví účet a zinkasuje platbu. Každý čip Smart Tags nese výrobcem zapsanou informaci o fyzických vlastnostech produktu, jemuž je přidělen (u oblečení to mohou být například data o barvě, velikosti a střihu, v potravinářském sortimentu zase informace o složení, původu, energetických hodnotách či době trvanlivosti jednotlivých potravinových výrobků), a jedinečný identifikační

kód. V současné době již řada firem takovéto „chytré štítky" zavádí a vzhledem k jejich užitečnosti lze předpokládat, že se tato technologie velmi rychle rozšíří.

V pasech

Podle některých informačních zdrojů budou RFID čip obsahovat také nové cestovní pasy obyvatel zemí Evropské unie. Miniaturní čip o tloušťce 0,06 milimetru a délce hran 0,4 mm integrovaný do cestovního dokladu bude pouhým okem prakticky neodhalitelný. Zakódovaná biometrická data majitele pasu umožní jeho rychlejší a spolehlivější identifikaci a díky tomu přispějí mimo jiné i k rychlejšímu nalezení či dopadení hledaných osob, nehledě k tomu, že nová technologie značně ztíží „práci" padělatelům.

Na bankovkách

Podobné RFID čipy se chystá implantovat do nových eurobankovek vyšších nominálních hodnot i Evropská centrální banka. Data budou na čipu uložena v modu „read-only", což zaručí jejich autenticitu a prakticky znemožní jejich následné přepisování. Dá se sice předpokládat, že dříve či později padělatelé přijdou na způsob, jak obelstít i tuto technologii, zatím se však čipová ochrana bankovek jeví jako nepřekonatelná.

Různé varianty

Společnost, která miniaturní RFID čipy vyvinula, samozřejmě disponuje jejich různými variantami. V případě bankovek je například pro úspěšnou komunikaci mezi čipem a čtečkou nutné, aby vzájemná vzdálenost nebyla vyšší než dva milimetry. V případě RFID čipu umístěného v cestovním dokladu bude operační dosah samozřejmě vyšší – až 300 mm.

Použitá literatura

[1] ŘÍHA, Milan; SIEGER; Ladislav, PIKOLA, Pavel: *Bezpečnostní systémy II.* Vydání druhé aktualizované. Námořní akademie České republiky. Praha 2011. ISBN 978-80-87103-35-7. Str. 148–153.

[2] KYNCL, Jaromír: *Ochrana zboží – elektronické a mechanické prvky.* In ABAS Report. Čís. 2. ABAS IPS Management. Ostrava 2009. Str. 7–9.

6.8 Detektory narušení (DN)

Milan Říha, Ladislav Sieger, Pavel Pikola
(pro potřeby této publikace upravil Jaromír Kyncl)

Detektory narušení, zvané též bezpečnostní čidla, představují tu část PZTS, která zjišťuje narušení prostoru. Pracují na různých principech, zejména na principu převodu specifického fyzikálního jevu, například přerušení elektrického obvodu, přerušení světelného paprsku narušitelem, na elektrický poplachový signál. K nejběžněji užívaným patří detektory magnetické, elektrické okruhy (signální stěny), radiolokační, termovizní nebo infračervené detektory, detektory využívající magnetické anomálie a vibrace. Dalšími pak jsou např. geofony, seismické detektory a podobná, finančně náročnější zařízení. Detektory narušení dnes nacházejí stále sofistikovanější uplatnění v ochraně obvodové, plášťové, prostorové i předmětové.

Magnetické detektory

Magnetické detektory patří k dostupným a jednoduchým zabezpečovacím prvkům, které nalézají široké uplatnění. Montují se do míst, kterými by nežádoucí osoba mohla vniknout do objektu (oken, dveří, poklopů, skleněných stěn, výkladních skříní apod.) Umisťují se také do stolů, skříní, vitrín (např. muzea) a jiných míst, která mají být zabezpečena před napadením. K vyhlášení poplachu dochází při změně vzájemné polohy spínače a ovládacího magnetu. Měly by být umísťovány s největším možným utajením. Jejich velikost bývá od několika milimetrů do pěti centimetrů s hmotností 15 až 40 gramů a s provozním napětím 12 či 24 V.

Bezdrátový magnetický detektor otevření

Výrobek je určen k detekci otevření dveří, oken apod. Detektor komunikuje bezdrátově a je napájen z baterie. Reaguje na oddálení magnetu. Vysílací díl se montuje na pevnou část dveří (okna) a magnet na pohyblivou část. Je třeba se vyhnout montáži přímo na kovové předměty, které negativně ovlivňují činnost magnetického senzoru i rádiovou komunikaci.

„Neviditelný" magnetický bezdrátový detektor otevření

Instaluje se přímo do rámu okna. Detektor se montuje do plastových či dřevěných rámů a lze jej použít u většiny typů kování. Napájí jej dvě knoflíkové lithiové baterie. Lze jej přiřadit do ústředny, do UC a AC přijímačů (ovládání

relé) a do sirény (indikace otevření zvukem). Detektor komunikuje bezdrátově protokolem OASIS a je napájen z baterií.

Roletový detektor

Slouží pro detekci (nežádoucí) manipulace s předokenní roletou, žaluzií a podobně. Připojuje se k bezdrátovému detektoru otevření, jehož součástí je univerzální vysílač. Speciální vstup pro vyhodnocování impulzů z roletového detektoru filtruje náhodné malé pohyby jeho lanka, například při poryvech větru, které mohou pohnout roletou. Jedná se v podstatě o rohatkový mechanismus, který při pohybu lanka, spojeného s roletou, střídavě rozpojuje a spojuje kontakt detektoru.

Záplavový detektor

Záplavový detektor slouží pro indikaci zaplavení prostor (sklepu, koupelny apod.) vodou. Tuto informaci lze zavést do zabezpečovacího systému a odeslat zprávu majiteli. Při propojení elektrod (zaplavením vodou) detektor vysílá signál aktivaci, zklidnění je vysláno, pokud propojení elektrod zmizí. Detektor je napájen přímo z obvodů bezdrátového detektoru otevření a pro svou činnost nepotřebuje jiný zdroj energie.

Rázové snímače

Reagují na určitý stupeň nárazu, který je možno nastavit na požadovanou citlivost. Především se používají všude tam, kde hrozí proniknutí do objektu skleněnými plochami, to znamená do výkladních skříní, skleněných dveří, oken apod.

Vibrační detektory

Generují napětí vznikající při vibracích piezoelektrického krystalu. Výstup piezokrystalu býval kombinován s frekvenčním filtrem, pomocí něhož lze nastavit citlivost a tím minimalizovat falešné poplachy, vniklé například poryvy větru, tlakovými vlnami apod. Zatím zřejmě nejdokonalejší prostředky pro detekci rozbití skla využívají jeho přetlaku, který vzniká při ohybu skla před rozbitím a následným tříštivým zvukem, přičemž tříštivost musí po ohybu následovat do 150 ms. To znamená, že vibrační detektor nenahlásí nebezpečí vniknutí, jestliže se třeba před výlohou rozbije skleněná láhev. Pokud je ale objekt osazen dvojskly, musí se instalovat speciální druhy vibračních detektorů.

Separátní vibrační detektory

Dokážou vyhlásit „tichý" poplach a vydávat signály, které umožní okamžitě lokalizovat místo narušení. Například při umístění v cenných uměleckých předmětech jsou schopny při jejich krádeži vyhlásit poplach, aniž by to zloděj tušil, a navíc po dobu, kdy je s předmětem pohybováno, tj. při útěku pachatele, označovat jeho polohu.

Tlakové senzory

Jsou využívány tam, kde je možno prostor alespoň částečně hermeticky uzavřít. Pracují na základě molekulárních změn ve vzduchových tlakových poměrech. To znamená, že při otevření dveří nebo oken takového uzavřeného prostoru dojde ke změně tlaku, který je schopen detektor zaznamenat. Protože zařízení nereaguje na pohyb osob uvnitř střeženého objektu, je vhodné jej použít i ve volně propojených místnostech a velkých prostorách, jako jsou kostely, školy, kulturní domy, prodejny apod.

Infračervené tepelné detektory

Pracují podobně jako termovizní kamery. Taktéž snímají obraz terénu a odlišují různá tepelná vyzařování objektů od pozadí. Tím vzniká tepelný obraz citelný buď v černobílé, nebo barevné verzi na obrazovce monitoru. Protože pro obsluhu zařízení by bylo neúnosné mnohahodinové sledování obrazovky, je kamera zapínána ve stanovených intervalech a jí pořízené obrazy jsou digitálně zaznamenávány. Ty je pak možno porovnávat s originálním obrazem prostředí uloženým v paměti řídicího systému. Přístroj sám muže automaticky vyhlásit poplach, shledá-li při narušení sledovaného prostoru změny. Dokonalejší systémy dovedou samy zjišťovat, zda odchylka obrazu odpovídá lidské postavě, automobilu či se jednalo například jen o průlet ptáka. Výhodou takových přístrojů je fakt, že jsou odolné proti elektromagnetickému rušení.

Infrapasivní detektory

Jsou založeny na podobném základu jako infračervené detektory. To znamená, že reagují podle nastavení přístroje na změnu infračerveného záření. Podle charakteru přístroje mohou buď samostatně vyhlásit poplach (samostatný hlásič), nebo narušení signalizovat do řídicí centra obsluze. V případě samostatného poplašného zařízení má detektor vlastní zdroj, nebo je napojen

na síť a tvoří kompaktní celek s osvětlovadlem či s akustickým poplachovým zařízením, případně s oběma. Takovéto detektory mají podle typu výrobku úhel záběru od několika, až do 360 stupňů. Jsou uzpůsobeny pro umístění na stěnách, stropech, v rozích místností i na zemi. V zájmu nenápadnosti se vyrábějí v různých velikostech a tvarech, jako třeba svítidla, užitkové předměty apod. Mají kontaktní nebo nastavitelnou snímací vzdálenost, a to od několika až do 40 metrů.

Bezdrátový detektor pohybu osob a destrukce skleněných ploch

Tento detektor v sobě sdružuje dva nezávislé detektory, PIR[8] snímač pohybu a duální senzor rozbití skla (rozezná rozbití okna do vzdálenosti 9 m). Digitální analýzou je dosažena vysoká odolnost k falešným poplachům. K detekci pohybu osob využívá PIR senzor. Rozbití prosklených ploch, které tvoří plášť chráněného prostoru, detekuje ze změn tlaku vzduchu a charakteristických zvuků rozbíjení skla. Detektor je určen do interiéru, komunikuje bezdrátovým protokolem a je napájen z baterií. Má také vstup pro připojení senzoru otevření dveří.

Poznámky k instalaci PIR detektoru

Před PIR senzorem nesmí být žádné překážky bránící jeho „výhledu" a nemá být instalován blízko kovových předmětů (stíní rádiovou komunikaci). Nejčastější příčinou nežádoucí aktivace detektoru bývá jeho nevhodné umístění. Tento detektor se nemá zapínat do střežení v době, kdy se v jeho prostoru pohybují lidé nebo zvířata. Lze ho montovat na stěnu nebo do rohu místnosti. V zorném poli PIR senzoru nemají být předměty, které rychle mění teplotu (elektrická kamna, plynové spotřebiče apod.), žádné předměty s teplotou blízkou lidskému tělu, které se pohybují (např. vlnící se záclony zahřáté radiátorem či sluncem) ani domácí zvířata. Detektor by neměl být montován proti oknům či reflektorům. V blízkosti detektoru rozbití skla nemá být vyústění vzduchotechniky, ventilátor ani jiné zdroje změn tlaku vzduchu nebo intenzivních zvuků. Ve střeženém prostoru též nemají být zdroje vibrací nebo rázů.

Tenzometrické detektory

Detekční princip tenzometrických detektorů je založen na vyhodnocování

[8] PIR – pasivní infračervené záření.

změny odporu, která je vyvolána manipulací se střeženým objektem. V oblasti poplachových zabezpečovacích systémů nacházejí uplatnění především jako prvky předmětové ochrany (např. muzejních exponátů), perimetrické ochrany a jsou taktéž použitelné jako elektronická ochrana prvků klasické ochrany. Využívají se převážně v následujících aplikacích:[9]

- závěsové detektory
- váhové detektory
- plotové detektory

Závěsové detektory

Jsou určeny pro střežení uměleckých předmětů ve výstavních síních, galeriích, muzeích. Podle nastavené citlivosti dokážou reagovat i na velmi nepatrné pohyby předmětu, či dokonce na pouhý dotyk. Princip aktivace jejich prvků umožňuje nepřetržitou činnost, tedy i v době běžného provozu. Zejména jsou vhodné do prostorů expozic, kam má přístup široká veřejnost. Na střežené předměty není zapotřebí nic připevňovat ani je nějak upravovat.

Váhové detektory

Váhový detektor se umísťuje pod střežený objekt (sošku, část nábytku aj.) a po připojení je zaznamenána výchozí hmotnost předmětu. Následně je již vyhodnocována každá její změna, tedy snížení i zvýšení hmotnosti.

Plotové detektory

Jde o detektory, které jsou určeny k perimetrické ochraně a systém střežení je založen na kombinaci mechanické a elektronické ochrany. Mechanická ochrana je tvořena žiletkovými, ostnatými nebo hladkými dráty, které jsou napnuty tak, aby při tahové změně došlo k aktivaci poplachu.

Moderní plotové detektory jsou většinou založeny na tzv. otřesových kabelech. Tyto kabely (někdy též nazývané mikrofonní) jsou připevňovány na plot a umožňují detekovat otřesy spojené s jeho přelézáním nebo prostříháváním. Dostupné otřesové kabely jsou obvykle založeny na různých typech

[9] BITALA, Petr; LICHOROBIEC, Stanislav; VESELÝ, Václav: *Elektromechanické detektory narušení.* In: LUKÁŠ, Luděk: Bezpečnostní technologie, systémy management I. VeRBum – Radim Bačuvčík. Zlín 2011. ISBN 978-80-87500-05-7. Str. 47–48.

indukce. Dalším existujícím řešením jsou akcelerometrické detektory zavěšované na plot a komunikující pomocí rádiového kanálu.[10]

Použitá literatura

[1] ŘÍHA, Milan; SIEGER; Ladislav, PIKOLA, Pavel: *Bezpečnostní systémy I.* Vydání čtvrté aktualizované. Námořní akademie České republiky. Praha 2011. Str. 26–33.

[2] BITALA, Petr; LICHOROBIEC, Stanislav; VESELÝ, Václav: *Elektromechanické detektory narušení.* In: LUKÁŠ, Luděk: Bezpečnostní technologie, systémy management I. VeRBum – Radim Bačuvčík. Zlín 2011. ISBN 978-80-87500-05-7. Str. 45–48.

[3] BURDA, Karel; LUTERA, Ondřej: *Venkovní detektory poplachových systémů.* In: ELEKTRO REVUE. Čís. 2. Sv. 14. Fakulta elektrotechniky a komunikačních technologií VUT v Brně. Brno 2012. Str. 2.

6.9 Biometrické systémy (BS)

Jaromír Kyncl

K tradičnímu uspokojování potřeb uživatelů přístupových a docházkových systémů slouží dosud klasické terminály využívající identifikaci osob pomocí kódů, kontaktních nebo bezdotykových karet a diskrétních čipů. Účelem těchto zařízení je prostřednictvím přístupových mechanismů a snímačů (vstupních turniketů, dveří s elektromagnetickým zámkem, závor, bran apod.) evidovat vstupy a průchody, kontroly docházky a návštěv, řízení vjezdů a výjezdů vozidel, monitorovat obchůzky, objednávání a výdej jídel nebo sledovat pohyb zboží ve skladech či materiálu ve výrobě. U složitějších přístupových a docházkových systémů s modulárně koncipovanými systémy je již možné zmíněné dění sledovat na počítači. Ostraha nebo jiný bezpečnostní subjekt má šanci konkrétní pohyb ihned případně také odepřít. Samozřejmostí je možnost propojení jednotlivých systémů PZTS (dříve EZS), EPS, CCTV a ACCESS CONTROL do integrovaných celků s jednotnou softwarovou nadstavbou, jež obsahují nezbytné aplikace pro uživatelské nastavení, správu systému a hlášení událostí. Výstupy z nich pak mohou sloužit jako podklad pro mzdovou evidenci. Pro aplikace, které vyžadují časové, stavové či jinak podmíněné řízení přístupu, jsou určeny volně programovatelné nadstavby. Díky nim je vcelku jednoduché připojit komplexní přístupový systém do internetové sítě a i na dálku nastavovat nová nebo rušit stávající oprávnění přístupu do objektů, monitorovat vstupy a vjezdy do objektu, jakož i přiřazo-

[10] BURDA, Karel; LUTERA, Ondřej: *Venkovní detektory poplachových systémů.* In: ELEKTRO REVUE. Čís. 2. Sv. 14. Fakulta elektrotechniky a komunikačních technologií VUT v Brně. Brno 2012. Str. 2.

vat systému mnoho dalších funkcí. Rychlý rozvoj slaboproudých technologií, inovace a trvalé snižování cen jejich konkrétních produktů umožňují pořizování novějších a především bezpečnějších terminálů. Majitelé firem se stále častěji zajímají o komplexnější a rozsáhlejší systémová řešení přizpůsobená na míru vlastním potřebám. Mnoho z nich si již uvědomilo, že používání různých hesel a osobních identifikačních čísel (PIN) přináší velká rizika při autorizaci, a tedy i snadnější zneužití neoprávněnou osobou. Téměř všechny starší způsoby identifikace osob (klíče, čipy, karty aj.), které dosud umožňovaly přístup do prostor většiny společností, jsou z těchto i mnoha dalších důvodů postupně nahrazovány mnohem spolehlivějšími systémy, dnes již realizovanými na principu využívání poznatků z oblasti biometrie.

Zvyšující se nároky na účinné zabezpečení kancelářských, výrobních, skladovacích a garážovacích prostor různých typů firem, společností a institucí nutí výrobce vyvíjet stále dokonalejší produkty. Přicházejí na trh s nabídkou spolehlivějších biometrických přístupových a docházkových terminálů, kterými je možno eliminovat dosavadní méně spolehlivé způsoby identifikace osob oprávněných ke vstupu do pracovních či privátních zón, případně k manipulaci se svěřenou technologií.

Biometrií obecně rozumíme souhrn výpočetních technik, který umožňuje rozpoznat jakoukoliv osobu na základě jejích anatomických parametrů, například otisků prstů, oční duhovky nebo sítnice, tváře, žilního řečiště, chůze, DNA či dynamiky podpisu. Tento souhrn dat je následně implementován do tzv. multimediálních biometrických snímačů. Ke snímání otisků prstů se nejběžněji používají optoelektronická, kapacitní, teplotní, elektroluminiscenční a radiofrekvenční zařízení. Vzhledem k faktu, že žádná z nich nejsou stoprocentně spolehlivá, jeví se v současné době jako nejúčinnější metoda snímání otisků prstu pomocí multispektrální zobrazovací technologie. Ta je schopna detekovat jeho vlastnosti i pod povrchem, navíc spolehlivě pracuje za extrémních podmínek okolního prostředí. Nevadí jí ani okolní světlo či výkyvy teploty, ani tekoucí voda, prach či jiné nečistoty. Ke zjevným slabinám tradičních snímačů patří odmítnutí identifikace z důvodu znečištění nebo poškození papilárních linií, vlivu statické elektřiny na životnost desky snímače, problémy se zpracováním algoritmů markantů či nesnadného vytváření databáze otisků. Protože existuje mnoho materiálů, ze kterých lze celkem snadno vytvořit umělý (falešný) otisk prstu, je nutno brát v úvahu i toto zvýšené riziko. Moderní multispektrální zobrazovací technologie využívá mimo jiné několika osvětlovacích soustav o rozdílných vlnových délkách. Světlo tak dokáže proniknout až pod povrch kůže, čímž umožní senzorům shromáždit

více identifikačních údajů z prstu a přesněji dotvořit obraz otisku. Dokáže též odhalit, zda má někdo na vlastním prstu nanesenou další organickou nebo syntetickou vrstvu (falzifikát). Rozezná i otisk z mrtvého člověka, neboť k její nesporné výhodě patří schopnost vyhodnocování momentálního stavu žilního řečiště. Nejmodernější verze multimediálních biometrických přístupových a docházkových terminálů jsou navíc vybaveny dotykovými obrazovkami, podporou bezdotykových ID karet, RFID (Radio Frequency Identification) čipů a grafickým rozhraním, umožňujícím zobrazování individuálních grafických ploch a osobních barevných fotografií. Většina funkcí podporuje přenos dat v reálném čase a má vícejazyčnou zvukovou podporu s možností přehrávání v mnoha formátech.

Použitá literatura

KYNCL, Jaromír: *Budoucnost biometrických přístupových systémů – hesla a osobní identifikační čísla minulostí*. In: Bezpečnost s profesionály. Čís. 3. KPKB ČR. Praha 2012. Str. 7.

7. OSTATNÍ BEZPEČNOSTNÍ SYSTÉMY

Jaromír Kyncl

Ostatní bezpečnostní systémy a výrobky jsou souborem technických a organizačních opatření, která mají chránit jakékoli majetkové nebo jiné hodnoty před odcizením, poškozením, zničením nebo jiným způsobem narušení. Kromě již zmíněných bezpečnostních technologií a systémů, které jsme stručně popsali v předchozí kapitole, a několika dalších, jež podrobněji zmíníme v této kapitole, se jedná o celou škálu systémů a výrobků, které s bezpečnostními technologiemi sice bezprostředně souvisejí, nebudou však předmětem užšího pojednání v této publikaci. Jedná se totiž o specializované elektroinstalace, kterým je věnována literatura zcela jiného odborného zaměření.

Jen pro zajímavost můžeme okrajově zmínit například silnoproudé elektroinstalace domů, bytů a kanceláří nebo instalace protinámrazové ochrany venkovních ploch. K slaboproudým elektroinstalacím patří zejména systémy příjmů pozemního, kabelového nebo satelitního televizního (rozhlasového) vysílání, rozvody pro domácí komunikační techniku, marketingové systémy analyzující obchodní chování zákazníků, systémy pro bezpečnostní a logistický monitoring vozidel, vyvolávací systémy pro odbavování osob na přepážkových pracovištích bank, poštovních úřadů, letišť, informačních center a úřadů či systémy hlídání dětí. Ke specializovaným činnostem patří také systém centrálního řízení času s přesným zdrojem (DCF, GPS) či systém propojování prostředků využívajících datovou komunikaci (počítačů) včetně periferních zařízení (tiskáren, IP telefonů aj.), přičemž se datové sítě liší zařazením do různých kategorií (například podle maximální rychlosti sítě) nebo provedením (drátové, bezdrátové WIFI, sítě s optikou). Skládají se z pasivní části, kterou nazýváme strukturovaná kabeláž, a aktivní části, jejímiž aktivními prvky jsou především datové přepínače, routery, modemy, konventory aj.[1]

[1] http://www.falcocomputer.cz/elektroinstalace/ezs-elektronicke-zabezpecovaci-systemy

V následujících kapitolách se budeme podrobněji věnovat těm bezpeč nostním systémům a výrobkům, které bezprostředně souvisejí s tématem naší publikace, tj. s bezpečností objektu.

7.1 Mechanické zábranné systémy

Milan Říha, Ladislav Sieger, Pavel Pikola

Nejjednodušší mechanické zábrany (kůly, provazové oplocení, nízké dřevěné nebo trubkové plůtky, živé ploty, závory) ve skutečnosti slouží pou ze k upozornění, že za nimi je soukromý pozemek a vstup tudíž není volný Zpravidla je toto zdůrazňováno i různými neoficiálními tabulkami s nápisy

Zábrany tvořené různými druhy vyšších plotů a zdí mají již úkol preven tivně zabránit snadnému fyzickému vstupu. Pro větší účinnost se u nich po užívá jako doplněk klasický ostnatý drát, tenká souvislá vrstva plochých a os trých plastikových ostnů zalisovaná do drátu či jenom zazděné kousky skla žiletek nebo hřebíků. U některých zvláštních objektů se uplatňuje navýšení zdí a plotů bariérou z ostnatého drátu připomínající nekonečnou srolova nou cívku nebo kovovou páskou s velmi ostrými hranami, na kterých jsou v malých roztečích ostny podobné žiletkám. Takové navýšení je až jeden met vysoké a svou řeznou plochou a samotným vzhledem vzbuzuje respekt. Ale ani to pro dobře připraveného a vycvičeného profesionála není při překoná vání takové zábrany vážným problémem. Proto jsou podobné mechanické zábrany kombinovány s elektronickými systémy.

Bezpečnostní folie na sklo

K mechanickým zábranám lze počítat i bezpečnostní folii aplikovanou na prosklené plochy. Svými vlastnostmi významně zpomaluje průnik narušite le do objektu. Tu dokonce považuje Česká pojišťovna na základě posudku Kriminalistického ústavu PČR za alternativu funkční mříže a uzamykatelné rolety. Jedná se o sklo obvykle silné 4 nebo 6 mm s nalepenou folií, která se vyrábí metodou tzv. „sputteringu", původně vyvíjenou pro potřebu kosmic kých letů. Folie jsou tvořené vrstvami polyesterového filmu a jsou silné 50 až 400 μm (= 0,05 až 0,4 mm). Folie jsou čiré a naprosto průhledné – pro pustnost světla se pohybuje kolem 90 %. Sklo opatřené touto bezpečnostní folií může sloužit jako velmi dobrá mechanická zábrana. Zpomaluje postup pachatele do objektu obdobně jako mříže, zamezuje prohození těžkých před mětů, dlažebních kostek, výbušnin a také zpomaluje šíření požáru. Základní surovinou pro bezpečnostní folie je vysoce čistý polyester. Na folii je nane

na vrstva disperzního lepidla s průsvitnou ochrannou folií, která se před montáží odstraňuje. Spojení folie se sklem je tím pevnější, čím větší silou je folie přitlačena na sklo. Sklo i folie musí být čisté a důležitá je i kvalita lepu.

Montáž folie na sklo je poněkud časově náročná, ale je jednoduchá. Na prosto čiré sklo se nastříká montážním roztokem a pak se na něj přiloží folie s provlhčenou vrstvou disperzního akrylátového lepidla. Pak se folie navlhčí a stěrkami se vytlačuje kapalina mezi sklem a folií až do dobrého přilnutí. Vytvrzení lepící vrstvy trvá až 6 týdnů. Folie se lepí na vnitřní stranu skla a musí zasahovat až na okraj skla.

Sklo

Skleněná výplň je nejslabším bezpečnostním článkem oken. Přes ni se uskutečňuje nejvíce průniků a proto je jí nutno věnovat potřebnou pozornost. Pro běžné zasklívání dřevěných oken se používají nejvíce plochá, tažená nebo tabulová plavená skla tloušťky 3 mm. Lze zasklívat i tepelně izolačními skly (dvojskla a trojskla). Skla jsou většinou průhledná, čirá, ale mohou být i matová, neprůhledná nebo s barevnými odstíny, s reflexními vrstvami či tlačeným vzorem. Do plochy skla může být zalité i drátěné pletivo, zamezující snadnému rozbití a proniknutí plochou okna. Sklo se do rámu upevňuje vložením do polodrážky v okenním křídle a následným upevněním tmelem, silikonem či jiným vhodným materiálem.

Pro zvýšení bezpečnosti oken se používá sklo:

tvrzené – např. sklo Restex, které je však vhodné spíše pro interiéry, pro svou tříštivost po úderu se nehodí na obvodové okenní otvory, používá se tam, kde jde o bezpečnost proti zranění (např. výplně vnitřních prosklených dveří apod.),

s bezpečnostní folií,

vrstvené – jde o sendvičovou technologii lepení skel, většinou ve vrstvách sklo-folie-sklo o tloušťkách 3-0,8-3 mm.

Mříže

jsou jednou z nejstarších mechanických zábran na světě vůbec a jejich po užívání je vyzkoušené uplynulými staletími. Používají se hlavně tam, kde majitelé či uživatelé nejsou trvale přítomni v budově či jejích částech, nebo v případě, že nechávají okna otevřená k větrání. Tomuto druhu zabezpečení

se zatím nedostalo pozornosti stanovením normativního základu na jejich výrobu, zkoušky a odolnost. Proto výrobci, zkušebny, klasifikují mříže dle potřebného času k jejich překonání. Mříží existuje velké množství druhů.

Dělíme je podle různých hledisek:

1) dle konstrukce:
   - pevně ukotvené,
   - odejímatelné,
   - otevírací (otočné, sklopné),
   - posuvné (pevné, nůžkové),
   - navíjecí (s průhledným průzorem, s neprůhledným průzorem),
2) dle umístění:
   - vnější – ploché nebo předsazené,
   - vnitřní, meziokenní,
3) dle materiálu:
   - ocelové, duralové,
   - z tvrzeného a šlechtěného hliníku,
4) dle ovládání:
   - ruční,
   - elektrické.

U každého druhu klademe důraz na funkci a spolehlivost. Bezpečnostním požadavkům na odolnost pevných mříží nejvíce vyhovuje tepelně zpracovaná ocel. U navíjecích mříží je důležitá hmotnost, proto se nejvíce využívá zušlechtěný hliník. Jedním ze základních požadavků je tuhost konstrukce. Ta musí být vysoká, mříže se nesmějí prohnout a oka roztáhnout. Zde záleží jak na použitém materiálu, tak na rozměrech a konstrukci. Právě konstrukce je zásadní. Spojení tyčí a prutů nesmí být rozebíratelné – to znamená žádné šrouby a nýty. Spojují se kvalitně provedenými sváry. U nůžkových posuvných mříží se spojují čepy. Je-li tedy mříž z kvalitního materiálu a dobře vyrobena je potřeba ji kvalitně a spolehlivě zasadit. Většinou se do zdi ukotvují přímo pruty a příčníky. Aby mříž odolala vytržení ze zdi, musí být ukotvena minimálně

14 cm do hloubky zdi. Pruty bývají zakončeny rozštěpem nebo jinou úpravou proti vytržení. Další možností zasazení je použití kovového mřížového rámu a na něj navařené kotvicí tyče. Dalším možným způsobem překonání mříží je prolézání. I když není příliš časté, musí na to být myšleno při konstrukci mříže. Velikost mřížového oka musí být max. 10 x 20 cm. Vzdálenost mezi vertikálními pruty má být max. 10 cm a největší vzdálenost mezi horizontálními příčníky 20 cm. Průřez vlastní použitou tyčí je min. 3,2 cm^2. To znamená u tyčí s kruhovým průřezem průměr 20 mm, u čtvercového průřezu 18 x 18 mm, u obdélníkového např. 16 x 20 mm. U posuvných nůžkových mříží jsou použity speciální U-profily s ocelovými nůžkami. Průměr použitých příčníků bývá kolem 15 mm, což je vyváženo větším počtem menších ok, a tím i větší pevností. Případný uzamykací systém, musí být taktéž v bezpečnostním provedení – u visacích zámků vytvrzené třmeny o průměru minimálně 12 mm.

Dveře

Dveře jsou statisticky nejpočetnějším místem vniknutí pachatele do objektu. Pod pojmem dveře je třeba si představit všechny jejich součásti: dveřní zárubeň, dveřní křídlo, uchycení dveří (závěsy), zárubeň, ochranné kování, vlastní zámek.

Zárubní se označuje rám, v němž jsou dveře zasazeny. Při stavebních úpravách objektu musí dojít k úpravě proti jeho roztažení. Při možnosti roztažení rámu ve výšce zámku vypadne totiž závora zámku ze zapadacího plechu a dveře se otevřou. Proto se zárubeň vylévá řídkým betonem, který po ztvrdnutí roztažení kovového rámu spolehlivě zabrání. Zapadací plech se proti vypáčení přichycuje dlouhými šrouby k zárubni. Nejlepším řešením a v případě státních objektů nejvíce používaným je namontování bezpečnostní zárubně. Jedná se o silné svařené kovové pásy, nebo ocelové profilované rámy. Pomocí kotevních čepů a háků zapadajících do ozubů brání násilnému vyražení zárubně ze zdi. Dalším krokem je použití bezpečnostních dveří. Bezpečnostní dveře jsou souhrnem speciálních stavebních, technických a bezpečnostních prvků a úprav dveřního prostoru, jenž zaručuje maximální bezpečnost chráněného objektu.

Zámek

Zvláštní pozornost je věnována rozličným způsobům bezpečnostního uzamykání vstupů do objektů. Ne všechny jsou totiž natolik kvalitní, aby odolaly zručnosti a vynalézavosti tzv. bytařů. Proto jsou tam, kde je to žádoucí, vcelku úspěšně instalovány dveřní bezpečnostní závory, dvojitá závora zamezující

vypáčení dveří, různá mechanická zajištění proti násilnému vysazení dveří, ocelové výztuhy ve dveřích a samozřejmě bezpečnostní zámky a jejich štíty. Ovšem i značně odolné zámky lze překonat odvrtáním, posunem závorek, vyplanžetováním či odtavením. To je však časově i profesionálně náročné. Proto se kvalita takového zabezpečení odborně posuzuje především podle doby nutné k jejich překonání. Není bez zajímavosti, že za zámky nižší kvality se považují ty, které je možno překonat do pěti minut, zámky střední kategorie jsou překonatelné do deseti minut a do nejvyšší kategorie patří takové mechanické bezpečnostní systémy, které vydrží odolávat útoku nad dvacet minut.

Poslední dobou se rozšiřuje používání zámku MULT-T-LOCK. Jedná se o zámek s třemi variantami klíče, které jsou barevně označeny (zelená, žlutá, červená). Přestane-li být první skupina klíčů vyhovující (z důvodu krádeže nebo ztráty), vsune se jednoduše do zámku jednoduše klíč druhé skupiny, kterým se po zamknutí a odemknutí přestavějí stavítka a první klíč již nelze použít. Totéž platí pro třetí (červenou) skupinu klíčů. Celý proces se dá po zásahu autorizovaného mechanika opakovat.

Důležitou částí zámku je uzamykací závora. Měla by být minimálně na dva západy, a v dostatečně masivním a širokém provedení pro zabezpečení zámku i zárubně. Nejbezpečnější je použití zámku s rozvorovým systémem. Jedná se o vícenásobné západy, kde závory zajišťují dveře na více místech. Závory jsou kulatého profilu s tloušťkou kolem dvou centimetrů. Počet použitých závor je velmi variabilní.

Žádná směrodatná norma nebo kategorizace zámkových zabezpečovacích zařízení však bohužel neexistuje. Musíme tedy vycházet z jednotlivých technických norem. Pro posouzení mechanické bezpečnostní úrovně dveřního prostoru je platná norma ČSN 747731 – dveře odolné proti vloupání. Stanovuje základní požadavky na bezpečnost, přičemž rozlišuje dvě kategorie. Kategorie A – zahrnuje výrobky z hlediska odolnosti s optimálními parametry, jež jsou srovnatelné s parametry mezinárodních norem. Kategorie B – požadavky na výrobky v této třídě jsou nižší než v mezinárodních normách. V této normě bohužel chybí pasáž o časovém intervalu, který je potřebný pro překonání dveří násilím. Chybí též parametry pro příčné závory a vícezávorové systémy. V tomto směru by měla pomoci připravovaná evropská norma EN 1630.

Použitá literatura

ŘÍHA, Milan; SIEGER; Ladislav, PIKOLA, Pavel: *Bezpečnostní systémy I.* Vydání čtvrté, aktualizované. Námořní akademie České republiky. Praha 2011. ISBN 978-80-87-105-32-6. Str. 11–14.

7.2 Mechanické zámkové systémy

Jaromír Kyncl

Zámek je mechanické zabezpečovací zařízení vyskytující se na dveřích, nábytku, vozidlech, nádobách apod. s cílem zamezit přístup k určitému majetku nebo do určitého prostoru. Zámek jako zabezpečovací zařízení se objevil již v Babylonu, kde archeologické nálezy potvrdily existenci dřevěných zámků s kovovým klíčem. Za dob antického Řecka a Říma se na původní funkci zámku mnoho nezměnilo, ale měnil se použitý materiál – zámky byly vyráběny z bronzu. Až do 17. století se vyráběly zámky, u kterých se dalo klíčem pouze pootočit, ale často jej nebylo možno ze zámku vyjmout. Během období renesance podléhaly zámky uměleckým vlivům. Byly zdobeny vysekávanými otvory, barevnými krytkami otvoru pro klíč nebo napouštěním (zbarvením oceli teplem). Zámky byly ještě „nezadlabané", pouze nasazené na vnitřní straně dveří.

Přibližně od poloviny 17. století se mechanismus zámků začal rychle vylepšovat. Významnou inovací byl patent Roberta Barrona z roku 1788. Jeho zámek byl již vybaven stavítky a pákami, které klíč musel zvednout do správné polohy. Barronův vynález dále vylepšil například Jeremius Chubb a později Robert Yale, který vynalezl v roce 1844 cylindrickou vložku, soustavu odpružených stavítek s blokovacími kolíky, která musely zuby klíče nastavit tak, aby bylo možno otočit cylindrem (válcem uvnitř zámku), jehož zub teprve dokázal pohnout závorou. Vznikl tak jednoduchý a subtilní, avšak bezpečný zámek, který poskytoval na tehdejší dobu značnou variabilitu klíčů.[2]

V průběhu 20. století prošel zámek dalším bouřlivým vývojem. Vycházel z profilových klíčů (renesance) přes dozické až po patentní (známé v Česku pod názvem FAB). Složitost zámků se postupně zvyšovala v zájmu zajištění bezpečnosti (bezpečnostní FAB, více stavítek atd.). Vznikla také bezpečnostní norma pro jednotlivé zámky.

Typy zámků podle užití:

- stavební (dveře, okna, rolety apod.),
- nábytkové,
- na dopravní prostředky.

[2] http://cs.wikipedia.org/wiki/Z%C3%A1mek_(za%C5%99%C3%ADzen%C3%AD)

Typy zámků podle systému:

- pevné, které se podle způsobu umístění na dveřích dále dělí na zadlabací (též zapuštěné), polozapuštěné a nasazené; v současnosti se vyrábějí prakticky jen zámky zadlabací; polozapuštěné a nasazené najdeme spíše u starožitných dveří, kdy mohl být mechanismus zámku velmi robustní a do dveřního křídla by se nevešel; v současné době se někdy na vstupní dveře přidává ještě bezpečnostní nasazený zámek, který se ovládá klíčem pouze z vnějšku, z vnitřní strany jej lze otevřít ručně;
- visací, u kterých je nevýhodou, že je lze poměrně snadno překonat přetržením nebo přepilováním, takže dnes se užívají především na dveře nižší kategorie (kůlny, nábytek apod.); jejich výhodou je, že je lze přenášet, protože nejsou nijak spojeny s dveřmi;
- lanové;
- speciální (elektronické, elektromagnetické).

Typy zámků podle otevírání:

- ruční,
- klíčové,
- mincové,
- kartové,
- heslové, jejichž výhodou je, že heslo si volí sám uživatel, takže je nemůže bez poškození otevřít ani výrobce zámku,
- dlaňové, otevírané přiložením dlaně, prstu, snímáním zorničky apod.

Použitá literatura

UHLÁŘ, Jan: *Technická ochrana objektů I. díl.* In: Mechanické zábranné systémy II. Policejní akademie České republiky. Praha 2009. ISBN 978-80-7251-312-3. Str. 11–12.

7.3 Systémy pro řízení evakuace

Jaromír Kyncl (vybrané pasáže z portálu Základy medicíny katastrof[3])

Evakuační systémy slouží pro zajištění rychlé a bezproblémové evakuace z prostor zasažených požárem či jinou mimořádnou událostí. Evakuace obyvatelstva je jedním z nejúčinnějších a nejrozšířenějších opatření, která se používají při ochraně obyvatelstva před případnými následky hrozících nebo vzniklých mimořádných událostí. Provádí se na základě předpokladu dlouhodobého či zásadního zhoršení životních podmínek vlivem přírodní katastrofy nebo i průmyslové havárie (radiační, chemické). Evakuační opatření se ve velké míře používají v době, kdy krizová situace hrozí, nebo je v počátečních fázích.

[3] http://zsf.sirdik.org/

Dělení evakuace

Z hlediska rozsahu opatření:

- evakuace objektová – zahrnuje evakuaci obyvatelstva jedné budovy nebo malého počtu obytných budov, administrativně správních budov, technologických provozů a dalších objektů;
- evakuace plošná – zahrnuje evakuaci obyvatelstva části nebo celého urbanistického celku, případně většího územního prostoru, plánuje se a rozlišuje na:
  - evakuaci všeobecnou, jíž podléhají všechny věkové kategorie osob (při živelních pohromách a průmyslových haváriích),
  - evakuaci částečnou, jíž podléhají některé nebo všechny následující kategorie (v některých případech vojenského ohrožení):

1) děti do 6let s individuálním doprovodem,
2) děti od 6 do 15 let se společným doprovodem,
3) pacienti zdravotnických lůžkových zařízení,
4) osoby přestárlé a osoby zdravotně postižené.

Z hlediska doby trvání:

- evakuace krátkodobá – ohrožení nevyžaduje dlouhodobé opuštění domova, pro evakuované se nezabezpečuje náhradní ubytování a nerealizují se opatření k zajištění nouzového přežití obyvatelstva;
- evakuace dlouhodobou – ohrožení vyžaduje dlouhodobý pobyt mimo domov, pro evakuované obyvatelstvo bez domova a bez možnosti vlastního ubytování je nutno zabezpečit náhradní ubytování a v potřebném rozsahu organizovat opatření k zajištění nouzového přežití obyvatelstva, pro zabez-

pečení jejich základních životních potřeb, popřípadě k zajištění ukrytí a individuální ochrany.

Z hlediska zvolené varianty řešení:

- evakuace přímá – prováděná bez předchozího ukrytí evakuovaných osob,
- evakuace s ukrytím – prováděná po předchozím ukrytí evakuovaných osob a po snížení prvotního nebezpečí.

Z hlediska způsobu realizace:

- evakuace samovolnou – není řízena a obyvatelstvo při krizové situaci jedná dle vlastního uvážení s cílem ubytovat se ve vlastních zařízeních, u příbuzných apod.; představitelé orgánů odpovědných za evakuaci a orgánů pověřených řízením evakuace se snaží získat kontrolu nad průběhem samovolné evakuace a snaží se ji v rámci možnosti usměrňovat tak, aby v nových místech ubytování neohrozili evakuovaní své zdraví a život a aby při přesunech nepřekáželi při provádění záchranných a likvidačních prací,
- evakuace řízená – představitelé orgánů zodpovědných za řízení evakuace tento proces řídí a ovlivňují; evakuované osoby se přemísťují vlastními dopravními prostředky, pěšky nebo dopravními prostředky hromadné přepravy zajištěnými orgány pověřenými řízením evakuace.

Způsoby varování a vyrozumění obyvatelstva

Včasné a kvalifikované zahájení realizace ochranných opatření v případech ohrožení obyvatelstva může výrazným způsobem zamezit poškození zdraví, ztrátám na životech a materiálním škodám. V rozhodující míře je založeno na včasném a správném předání varovných informací. Význam varovných informací je o to větší, že zejména na začátku mimořádných událostí je činnost obyvatelstva ve velké míře realizována svépomocí nebo vzájemnou pomocí.

Varování obyvatelstva je zejména úkolem státu, zastupovaného především Hasičským záchranným sborem ČR, dále je záležitostí obcí a provozovatelů jaderných zařízení, dále potom zaměstnavatelů (vůči svým zaměstnancům), vedení škol (vůči svým žákům, studentům), správy úřadů, nemocnic, ústavů a obdobných zařízení (vůči svým klientům) apod.

Podle zákona č. 239/2000 Sb. (§ 7 písm. f) zajišťuje a provozuje Ministerstvo vnitra ČR jednotný systém varování a vyrozumění, stanoví způsob informování právnických a fyzických osob o charakteru možného ohrožení, o připravovaných opatřeních a způsobu a době jejich provádění. Vyhláška Ministerstva vnitra č. 380/2002 Sb., k přípravě a provádění úkolů ochrany obyvatelstva (§ 4–11), stanovuje technické, provozní a organizační zabezpečení jednotného systému varování a vyrozumění.

Technicky, provozně a organizačně je systém varování v České republice zabezpečen vyrozumívacími centry, telekomunikačními sítěmi a koncovými prvky varování a vyrozumění, jako jsou elektronické sirény, elektronické rotační sirény nebo obecní rozhlasy.

Obyvatelstvo je v případě hrozby nebo vzniku mimořádné události varováno především prostřednictvím varovného signálu „Všeobecná výstraha" – ten je charakterizován kolísavým tónem sirény po dobu 140 vteřin a může zaznít třikrát po sobě v cca tříminutových intervalech. Okamžitě po doznění tohoto signálu následuje mluvená tísňová informace, kterou se obyvatelstvu sdělují údaje o bezprostředním nebezpečí vzniku nebo o již nastalé mimořádné události a o opatřeních k ochraně obyvatelstva. K poskytování této tísňové informace se využívá i tzv. koncových prvků varování, které jsou vybaveny modulem pro vysílání hlasové informace.

Dalším signálem, který sirény mohou vysílat je „Požární poplach", který slouží ke svolání jednotek požární ochrany. Tento signál je vyhlašován přerušovaným tónem sirény po dobu 1 minuty.

První středu v měsíci probíhá na celém území republiky „akustická zkouška" provozuschopnosti celého systému varování. Přesně ve 12:00 hodin se sirény rozeznívají zkušebním nepřerušovaným tónem po dobu 140 sekund, u elektronických sirén jsou občané vyrozuměni také hlasově. Signál generovaný elektronickou sirénou nebo rozhlasem doplňuje verbální zpráva. Jedná se o krátkou asi dvacetisekundovou informaci, která je uvozena na jejím počátku a na konci gongem. Verbální informace mohou být reprodukovány po zaznění signálu nebo i samostatně.[4]

[4] VOTÍPKA, Luboš: *Jednotný systém varování a informování.* In: Security magazín. Praha 2012. Čís. květen, červen 2012. Str. 18.

Tísňové informování obyvatelstva

Tísňové informování obyvatelstva lze chápat jako souhrn organizačních, technických a provozních opatření, která povedou k předání informací bezodkladně po zaznění varovného signálu o zdroji, povaze a rozsahu nebezpečí a po nutných opatřeních k ochraně života, zdraví a majetku, a to především cestou hromadných informačních prostředků (veřejnoprávních i lokálních médií), ale i dalšími způsoby.

Informování obyvatelstva organizuje a za obsah informací zodpovídá ten, kdo nařídil varování obyvatelstva daného území. Provozovatelé hromadných sdělovacích prostředků jsou povinni tísňové informace odvysílat.
Pro předávání informací lze využít:

- televizní a rozhlasové stanice s celostátní působností – Generální ředitelství Hasičského záchranného sboru má smluvně zajištěno vysílání na ČT 1, ČT 2 a ČRo 1 Radiožurnál,
- soukromé regionální rozhlasy a televizní společnosti,
- městské, obecní a objektové rozhlasy,
- elektronické sirény – jsou schopny vysílat informace prostřednictvím vlastního mikrofonu nebo z externího zdroje modulace (např. VKV-FM, rozhlasového přijímače, radiostanice),
- mobilní rozhlašovací prostředky (např. rozhlasové vozy, megafony),
- vozidla Hasičského záchranného sboru ČR a Policie ČR vybavená výstražným rozhlasovým zařízením.

Evakuační zavazadlo

Evakuační zavazadlo se připravuje pro případ opuštění bytu v důsledku vzniku mimořádné události nebo nařízené evakuace. Jako evakuační zavazadlo poslouží lehké cestovní zavazadlo např. batoh, cestovní taška nebo kufr, opatřené jménem a adresou majitele.

Doporučený obsah evakuačního zavazadla:

- osobní doklady (občanský průkaz, cestovní pas, rodný list, řidičský průkaz, průkaz pojištěnce, oddací list, doklady o ukončeném vzdělání, rozhodnutí o přiznání starobního důchodu, pojišťovací smlouvy, doklady od vozidla, psací potřeby),

- léky a zdravotní pomůcky (osobní léky, obvazy a další vybavení běžné lékárničky), brýle ke čtení aj.,
- cennosti (peníze, vkladní knížky, cenné papíry, smlouvy o stavebním spoření, penzijním a životním pojištění, platební karty),
- sezonní oblečení (náhradní oděv, prádlo, pláštěnka),
- přiměřená zásoba prostředků osobní hygieny a hygienických potřeb,
- spací pytel (přikrývka), karimatka, nafukovací lehátko,
- jídelní nádobí, šicí potřeby, kapesní nůž, otvírač na konzervy,
- základní (trvanlivé) potraviny na 2–3 dny (těstoviny, rýže, ovesné vločky, krupice, suchary, balený chléb, tavený sýr, kondenzované mléko, hotové a instantní potraviny, masové konzervy, rybí konzervy, konzervovaná zelenina, trvanlivé uzeniny, luštěniny, cukr, med), včetně nápojů (minerální voda a další nápoje v plastových lahvích, rozpustná káva),
- kapesní svítilna a náhradní baterie, svíčky, zapalovač, zápalky,
- mobilní telefon a nabíječka,
- přenosný rozhlasový přijímač a náhradní baterie, píšťalka, předměty pro vyplnění dlouhé chvíle (knížka, společenská stolní hra),
- pro případ evakuace s domácím zvířetem – zdravotní průkaz domácího zvířete a vhodná schránka nebo jiné zabezpečení pro jeho převoz.

Použitá literatura

[1] Zákon č. 239/2000 Sb., o integrovaném záchranném systému.

[2] Vyhláška Ministerstva vnitra č. 380/2002 Sb., k přípravě a provádění úkolů ochrany obyvatelstva.

[3] Vyhláška Ministerstva vnitra č. 328/2001 Sb., o některých podrobnostech zabezpečení integrovaného záchranného systému.

[4] NAVRÁTIL, Leoš; ŠAFR, Gustav; HAVRÁNKOVÁ, Renata; NAVRÁTIL, Václav; SIROVÝ, Ladislav: *Varování a vyrozumění obyvatelstva*. In: Základy medicíny katastrof. Kapitola 3.1.2 (http://zsf.sirdik.org).

[5] NAVRÁTIL, Leoš; ŠAFR, Gustav; HAVRÁNKOVÁ, Renata; NAVRÁTIL, Václav; SIROVÝ, Ladislav: *Evakuace obyvatelstva*. In: Základy medicíny katastrof. Kapitola 3.1.4 (http://zsf.sirdik.org).

[6] VOTÍPKA, Luboš: *Jednotný systém varování a informování*. In: Security magazín. Praha 2012. Čís. květen, červen 2012. ISSN 1210-8723. Str. 18.

7.4 Systémy nouzového osvětlení

Jaromír Kyncl

Podobně jako v každém odvětví bezpečnostních technologií a systémů hrají v posledních několika letech také v oboru systémy nouzového osvětlení hrají v posledních několika letech důležitou roli nové výrobky a nejrůznější řešení. Nouzové osvětlení se dělí podle účelu na náhradní osvětlení a nouzové únikové osvětlení. Náhradní osvětlení není bezprostředně určeno pro nouzové únikové osvětlení Přesnější kategorizace specifikuje nouzové osvětlení jako osvětlení únikových cest, protipanické osvětlení a nouzové osvětlení prostorů s velkým rizikem.

Nouzové únikové osvětlení slouží jako:

- nouzové osvětlení požárního zařízení (hlásičů, hydrantů) – je řízeno samostatně; napájeno je buď z centrální baterie nebo z autonomních akumulátorů umístěných přímo ve svítidlech a spouští se pouze na pokyn zařízení EPS (elektrické požární signalizace),
- nouzové osvětlení označených únikových cest – spouští se při výpadku napájení objektu; pro osvětlení únikových cest se používají svítidla, která osvětlí jak celou únikovou cestu, tak případný piktogram s označením směru úniku,
- značení únikových cest – spouští se rovněž při výpadku napájení objektu; jedná se o tzv. podsvětlené piktogramy s vyznačením směru úniku; úkolem svítidel není únikovou cestu osvětlit, ale jasně a viditelně ukázat směr úniku.

Z hlediska napájení se nouzové soustavy dělí na dvě hlavní skupiny:

1) soustavy, které jsou napájeny autonomními akumulátory umístěnými v jednotlivých svítidlech,
2) soustavy, které jsou napájeny z centrálního akumulátorového zdroje.

V obou případech by měla být svítidla bezpečnostního osvětlení napojena na centrální monitorovací systém, který umožňuje z jednoho bodu svítidla nouzového osvětlení řídit a současně provádět a vyhodnocovat periodické testy funkčnosti a autonomie a zjišťovat možné poruchy na svítidlech.[5]

[5] Kolektiv pracovníků EXX, s.r.o.: *Nouzové osvětlení – srovnání s centrálním zdrojem a s decentralizovanými akumulátory.*

Nouzově osvětlené prostory

Podle níže uvedených norem pro nouzové osvětlení musí být v každém objektu osvětleny:

- únikové cesty
- protipanické prostory
- zvláště nebezpečné prostory

Nouzové osvětlení tvoří klíčovou část osvětlovací soustavy, která je zodpovědná za umožnění bezpečné evakuace osob z ohrožených budov nebo jejich částí. Pro ohrožení života, zdraví osob a majetku v objektech pro shromažďování a ve výškových budovách je nejnebezpečnější vznik požáru a nedokonalé zabezpečení evakuace osob z ohrožených částí objektů, v nichž došlo k nebezpečné situaci. Z toho vyplývají jasné požadavky na maximální spolehlivost zařízení použitých pro účely bezpečného opuštění postižených prostorů, jež jsou definované minimálně těmito základními normami:

- ČSN EN 1838. Světlo a osvětlení – Nouzové osvětlení – stanovuje světelně-technické požadavky na soustavy nouzového osvětlení; dále doporučuje umístění nouzových protipanických a nouzových únikových svítidel;
- ČSN EN 50172. Systémy nouzového únikového osvětlení – stanovuje požadavky na kontrolu systémů nouzového osvětlení, předepisuje způsob a četnost pravidelných testů a zavádí povinnost vést provozní deník;
- ČSN EN 50171. Centrální napájecí systémy – předepisuje požadavky na centrálně napájené systémy nouzového osvětlení, jejich technické parametry a stanovuje minimální požadavky na konstrukci těchto systémů;
- ČSN EN 50272-2. Bezpečnostní požadavky pro akumulátorové baterie a akumulátorové instalace – část 2: Staniční baterie – stanovuje požadavky na bezpečnost bateriových systémů, jejich instalaci, provozní podmínky, kontrolu, servis a výměnu baterií.

Použitá literatura

[1] Kolektiv pracovníků EXX, s.r.o.: *Nouzové osvětlení – srovnání s centrálním zdrojem a s decentralizovanými akumulátory.* In: Světlo – časopis pro světlo a osvětlování. Čís. 5. Praha 2009. On-line verze časopisu Světlo. ISSN 1212-0812. Str. 22.

[2] ČSN EN 1838. Světlo a osvětlení – Nouzové osvětlení

[3] ČSN EN 50172. Systémy nouzového únikového osvětlení

7.5 Průmyslová havarijní signalizace

Jaromír Kyncl

Podle zákona č. 59/2006 Sb., o prevenci závažných havárií, je provozovatel objektu povinen provést pro účely zpracování bezpečnostního programu nebo bezpečnostní zprávy analýzu a hodnocení rizik závažné havárie, kde se uvádí:

a) identifikace zdrojů rizika (nebezpečí),

b) určení možných scénářů událostí a jejich příčin, které mohou vyústit v závažnou havárii,

c) odhad dopadů možných scénářů závažných havárií na zdraví a životy lidí, hospodářská zvířata, životní prostředí a majetek,

d) odhad pravděpodobností scénářů závažných havárií,

e) stanovení míry rizika,

f) hodnocení přijatelnosti rizika vzniku závažných havárií.

K nejznámějším a nejčastějším objektům a zařízením s možným rizikem závažné havárie řadíme zejména[6]:

- objekty a zařízení s čpavkem – s množstvím od 3 t mohou následky potenciální havárie přesáhnout vzdálenost 100 m (zimní stadiony, pivovary, mlékárny, masokombináty),
- objekty a zařízení s chlorem – s množstvím od 0,3 t mohou následky potenciální havárie přesáhnout vzdálenost 100 m (úpravny vod),
- objekty a zařízení s LPG – s množstvím od 10 t mohou následky potenciální havárie přesáhnout vzdálenost 100 m (autocisterny, železniční cisterny).

Detekce havarijních stavů

Podstatou většiny detekčních systémů je čidlo, které kontinuálně snímá definované parametry ve sledovaném prostoru. Čidla pracují na různých fyzikálních principech, například polovodičových, katalytických či elektrochemických. Detekční přístroje jsou vybaveny elektronikou, která vyhodnocuje stav čidla a zároveň plní požadavky na spínání dalších elektrických obvodů

[6] BERNATÍK, Aleš: *Prevence závažných havárií I.* Sdružení požárního a bezpečnostního inženýrství se sídlem VŠB – TU Ostrava. Ostrava 2006. ISBN 80-86634-89-2. Str. 22, 80.

a výkonných prvků bezpečnostních systémů. Základní výstražnou a havarijní ochranu průmyslových, zemědělských či jiných objektů představují stacionární i mobilní systémy detekce úniku plynů a par organických látek. Mohou tvořit jakýsi předstupeň vyšších systémů EPS či MaR (měření a regulace), avšak svými perifériemi umožňují i samostatnou varovnou činnost či možnost případného řízení technologií.

K dalším nezbytným detektorům používaným v průmyslových zařízeních a objektech patří snímače přítomnosti plynu v nevýbušném prostředí, snímače přítomnosti plynu pro průmyslové aplikace s nebezpečím výbuchu, záplavová a hladinová čidla, teplotní senzory, senzory pro signalizaci úniku nebezpečných chemických a ropných látek, kompaktní detektory požáru, havarijní ventily potrubních systémů, kotlů a čerpadel, spínače k vypnutí elektrického napájení, nebo spínače k automatickému odstavení strojů a výměníkových stanic.

K varování zaměstnanců a obyvatelstva v zóně případného výskytu havárie jsou určeny:

- koncové prvky JSVV (jednotného systému vyrozumění a varování),
- elektrické rotační sirény,
- osobní vyrozumění,
- mobilní vyhlašovací prostředky obsluhy jednotky HZS, Policie ČR,
- mobilní vyhlašovací prostředky vozů Policie ČR (vozidla vybavená výstražným signalizačním a rozhlasovým zařízením),
- regionální rozhlasové a televizní vysílání – umožňuje plošnou informovanost a varování obyvatelstva na ohroženém území při vzniku havarijní události,
- kabelová televize.

Použitá literatura

[1] Zákon č. 59/2006 Sb., o prevenci závažných havárií.

[2] Nařízení vlády č. 254/2006 Sb., o kontrole nebezpečných látek.

[3] Vyhláška č. 255/2006 Sb., o rozsahu a způsobu zpracování hlášení o závažné havárii a konečné zprávy o vzniku a dopadech závažné havárie.

[4] Vyhláška č. 256/2006 Sb., o podrobnostech systému prevence závažných havárií.

7.6 Zdravotnické signalizační a komunikační systémy

Jaromír Kyncl

Zdravotnické signalizační a komunikační systémy jsou používány ze jména na lůžkových odděleních nemocnic, v domovech důchodců, a jiných zdravotnických zařízeních a dnes již například i v hotelových komplexech. Možnosti těchto systémů už dávno nekončí rozsvícením signálního světla a akustickým signálem, i když jsou samozřejmě instalace, kde má i toto opatření své opodstatnění. Dnešní signalizační a komunikační systémy umožňují díky moderním technologiím sdružovat pod jeden celek více jednotlivých oddělení se samostatným provozem během dne a jejich sloučení pro noční či víkendový provoz s plnohodnotným zástupem jednotlivých oddělení navzájem, což umožňuje šetřit provozní náklady. Systémy umí rozlišit standardní a nouzové volání, komunikaci zdravotnického personálu mezi sebou. Existuje i možnost IP nadstavby a také bezdrátových přenosných terminálů pro lékaře i sestry. Samozřejmostí je záznam o délce jednotlivých volání, o historii událostí a možnost dálkové správy po LAN síti. Nabízená zařízení umožňují mimo jiné obousměrné hovorové spojení pacient – ošetřující personál či ošetřující personál – lékař, dále nouzová a poplachová volání, centrální hlášení, poslech zábavného programu, telefonní spojení s veřejnou telefonní sítí atd.

K nejznámějším a cenově nejdostupnějším patří osobní mobilní rádiové vysílače tísňového volání. Jsou určeny k ochraně zaměstnanců v rizikových provozech, jakými jsou například nápravná zařízení, psychiatrické kliniky, ambulance, detenční ústavy nebo uzavřená oddělení nemocnic. Vysílače je možno nosit na krku nebo na svazku klíčů, jsou nárazuvzdorné a voděodolné. Neobsahují žádné pohyblivé části a jejich napájení je zajištěno jednou vyměnitelnou úspornou alkalickou baterií, která vydrží zhruba 3 roky. Vysílače jsou vybaveny tlačítkem „Panika" pro přivolání okamžité nejbližší pomoci. Stisknutím tohoto tlačítka vyšle ovladač rádiový signál a kódovanou IR zprávu pro přesnou lokalizaci a identifikaci napadané (kolabující) osoby.

Popis některých základních funkcí nouzové zdravotnické signalizace komunikace:[7]

- monitorování zdravotního stavu uživatele – rozpoznání akutních zdravotních rizik, stavu nouze;
- automatická analýza dat – snímací jednotka obsahuje integrované sníma-

[7] http://www.andelstrazny.eu/cs/domaci-tisnova-pece/

ní pohybové aktivity uživatele, a umožňuje tak i bez signalizace ze strany uživatele rozpoznat některé krizové stavy (například případ náhlého pádu apod.) a včasnou reakcí předcházet následným komplikacím;

- tísňové volání – stiskem SOS tlačítka na alarmu nebo stiskem přenosného bezdrátového vodotěsného tlačítka je odeslána nouzová SMS až na tři čísla a je aktivováno volání až na pět čísel; další tísňová tlačítka je možno doplnit, může být tedy být instalováno např. v koupelně pro případ pádu apod.;
- připomínání odběru léků – možnost nastavení až čtyř časů, ve kterých ústředna akusticky signalizuje čas podávání léků;
- jednoduchá a přehledná správa – nabízené systémy jsou rozšiřitelné o možnost napojení na PC a velkoplošný informační panel,
- oboustranná hands-free hlasová komunikace – umožňuje v případě vzniklé tísňové situace na dálku verbální kontakt mezi postiženým a dispečinkem; příchozí volání z nastavených čísel jsou automaticky přijímána, okamžitě se zahájí hlasitý hovor; hlídaná osoba tak nemusí ani vstát z lůžka;
- rychlé vytáčení – do systému lze uložit až 3 telefonní čísla, která se po stisku tlačítka aktivují; lze okamžitě hovořit s předvolenými účastníky;
- monitoring pohybových aktivit – možnost instalace až čtyř bezdrátových detektorů; pokud není v nastavené době detekován pohyb, jsou odeslány nouzové SMS na definovaná čísla; lze tak snadno ohlídat, jestli byl hlídaný pacient během poledne v kuchyni, večer v koupelně atd.; pokud například nevstane celý den z lůžka, je automaticky odeslána SMS na dispečink;
- monitoring domácího bezpečí – k ústředně lze nainstalovat např. požární čidla, která zajišťují střežení po dobu 24 hodin; v případě poplachu jsou odesílány nouzové SMS;
- monitoring napájení – v případě výpadku síťového napájení a provozu ze záložního akumulátoru zašle SMS zprávu, provoz na záložní akumulátor by měl vydržet minimálně 12 hodin.

7.7 Nouzové zvukové systémy

Jaromír Kyncl

Nouzový zvukový systém je systém pro zesílení nebo distribuci zvuku, který se používá pro rychlou a organizovanou evakuaci obyvatel při nouzových situacích. Používanější neoficiální název je „evakuační rozhlas". Pokud jde o systém používaný k řízení evakuace při požáru, používá se často název „požární rozhlas". Nouzový zvukový systém může plnit i další funkce, jako je přenos hudby a informačních hlášení. Zvukový systém pro nouzové účely musí umožňovat vysílání srozumitelné informace o opatřeních, která je za potřebí uskutečnit k ochraně životů v jedné nebo více stanovených oblastech.

Ve školách, úřadech a jiných veřejných budovách je mnohdy výhodnější použít v případě nebezpečné situace (např. při požáru v budově) konkrétní mluvené hlášení. Tuto úlohu dokáže automaticky zajistit evakuační rozhlas propojený se systémem PZTS. Systém evakuačního rozhlasu podléhá certifikaci podle ČSN EN 54-16 a jeho montáž a provoz se řídí vyhláškou č. 246/2001 Sb., o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru (vyhláška o požární prevenci).

Základní skladbu nouzového zvukového systému tvoří tyto prvky:[8]

- řídicí systém – ústředna,
- zónový přepínač/matice,
- provozní zesilovač,
- záložní zesilovač,
- záložní napájecí zdroj s akumulátory,
- kontrolované vedení pro reproduktory,
- vedení pro mikrofonní pulty; u pultů určených k vyhlašování evakuace musí být kontrolované včetně vlastního mikrofonu,
- koncové prvky – mikrofonní pulty, reproduktory.

Mezi základní funkce nouzového zvukového systému patří:

a) informovanost o ohrožení,

b) pomoci navést osoby k únikovým cestám, k rychlému opuštění nebezpečné oblasti.

[8] http://www.avalon.cz/produkty/nouzovy-zvukovy-system.htm

Nouzový zvukový systém má také funkce doplňkové:

- prezentaci provozních hlášení,
- distribuci hudby na pozadí,
- reklamní sdělení.

Je-li detekován poplach, musí nouzový zvukový systém vyřadit všechna ostatní hlášení, vysílaná do zón reproduktorů nouzového zvukového systému. V praxi to znamená, že je-li nouzový zvukový systém využíván i pro informační, zábavné a reklamní hlášení, musí mít nouzové signály vždy největší prioritu – musí tedy při zahájení nouzového hlášení veškeré modulační zdroje automaticky odpojit.

Spolupracuje-li nouzový zvukový systém se systémem elektrické požární signalizace, případně je-li v dokumentaci požárního zabezpečení uveden jako zařízení k vyhlašování požárního poplachu, je zároveň normami požárního zabezpečení staveb definován jako technické zařízení k řízení evakuace, případně jako zařízení sloužící k protipožárnímu zabezpečení stavebních objektů a vztahují se na něj i normy řady ČSN 7308-(xx). Požární bezpečnost staveb.

Použitá literatura

[1] ČSN EN 60849. Nouzové zvukové systémy.

[2] ČSN EN 54-24. Komponenty pro hlasové výstražné systémy – reproduktory.

[3] ČSN EN 54-16. Ústředny pro hlasová výstražná zařízení.

7.8 Pochůzkové systémy

Jaromír Kyncl

Současné moderní pochůzkové[9] systémy se používají jako náhrada za dřívější knihy pochůzek. Princip fungování je velmi jednoduchý. Do všech míst, která je potřeba sledovat, se nainstaluje speciální čip. K tomuto čipu pak pracovník ostrahy přiloží čtecí zařízení (například přenosný elektronický snímač PES® Control System, dále jen PES®), které obsahuje jedinečnou identifikaci strážného. Automaticky se načte přesné datum, čas a místo kontrolního bodu. Poté lze tato data ze čtecího zařízení přenést a vyhodnotit na PC.

[9] Pravidelně konaná pochůzka strážného (hlídače) za účelem kontroly (Ústav pro jazyk český Akademie věd ČR, v.v.i.).

Klíčové vlastnosti snímačů PES®:[10]

- ergonomický design – malý rozměr (90 mm) a hmotnost (49 g) snímače PES® spolu s dalšími konstrukčními vlastnostmi ze snímače PES® velmi chytrý, bezpečný a uživatelsky pohodlný nástroj kontroly činnosti zaměstnanců;
- technologie ANTI-VANDAL® – celosvětově unikátní systém ochrany snímačů PES® před všemi možnými druhy poškození; ANTI-VANDAL® umožňuje detekovat a zaznamenat pokusy o zničení snímače a díky této technologii se snímače PES® právem řadí k nejodolnějším na trhu,
- kapacita – snímače PES® poskytují kapacitu zápisu až 14 000 událostí,
- nízké provozní náklady – pětiletá záruka a desetiletá životnost baterie zaručují uživateli nízké náklady na provoz systému.
- široké možnosti uplatnění v řadě odvětví lidské činnosti – kontrola strážných a strážní služby, revize zařízení, kontrola oprávněnosti přístupu do objektu, poštovní služby, úklidové služby a mnohé další,
- tři typy snímačů – PES Profi, PES Forte, PES Mini – s různými parametry a v různých cenových kategoriích,
- software WinKontrol™ – uživatelsky přívětivý software pro snadné zpracování načtených dat; umožňuje tvorbu celé řady výpisů.

Široké spektrum možností použití nabízí také systém pochůzkový systém Active Guard, který je unikátní tím, že umožňuje skloubit moderní způsob přenosu dat v reálném čase a tradiční ukládání dat. Ve spolupráci s moderním webovým portálem PATROLCONTROL tak uživatel získává okamžitý přehled o všech událostech, alarmových stavech a monitorovaných osobách. Výhody systému Active Guard:

- komunikace v reálném čase (GPRS/GSM),
- poplachové tlačítko „Panika“,
- spolehlivý a bezpečný provoz, kódování pomocí algoritmu DES,
- oboustranná hlasová komunikace – již žádné mobilní telefony na pracovišti,
- jednoduché ovládání (jen tři tlačítka),

[10] http://www.tomst.com/site/docs/PES000101CZ.pdf

- větší bezpečnost pro strážné i pro objekt,
- mnohonásobně vyšší garance odolnosti systému než u alternativních produktů v podobě PDA či mobilních telefonů.

Vyhodnocení probíhá ihned, tzn., že v okamžiku načtení bodu je informace odeslána do příslušného vyhodnocovacího softwaru (tzv. on-line), nebo se ukládá ve snímači až do jeho vyčtení a vyhodnocení kontrolním pracovníkem (tzv. off-line).

Základní charakteristika portálu PATROLCONTROL:[11]

- zobrazení dat a práce s portálem v libovolném webovém prohlížeči,
- možnost využití portálu více uživateli se systémem omezení a práv,
- obsahuje databáze uživatelů, zákazníků, objektů, snímačů, strážných (skupin strážných), kontrolních bodů a tras,
- jednoduché a přehledné menu,
- aktivní pohled na aktuálně načtené kontrolní body a poplachové zprávy,
- přehledná tabulka snímačů, včetně zobrazení stavových ikon,
- rozlišení kontrolních bodů dle využití (kontrolní bod, dynamický bod, poplachový bod) a jejich přiřazení k objektům,
- snadné plánování pochůzek a přímý tisk plánu pochůzek pro ostrahu,
- široký rozsah nastavení při plánování pochůzek, monitoring pochůzek,
- možnost výběru individuálního chování každé poplachové, nebo informační zprávy,
- přímé propojení portálu PATROLCONTROL s DPPC pro detailnější práci s poplachovými událostmi,
- upozornění na technické poplachy (otevření krytu baterie, náraz ve smyslu indikace signálu pro nouzový stav tzv. „mrtvý muž“, slabá kapacita baterie),
- zobrazení upozornění při požadavku na zpětné zavolání,
- okamžitá informace při nezahájení nebo nekorektním provedení pochůzky,
- automatická kontrola správnosti provedených pochůzek,

[11] http://dobraagentura.cz/?page_id=268

- využití čipu strážného,
- operátor má pro řešení poplachů po ruce všechny kontaktní informace,
- zobrazení GPS pozice zařízení (snímačů s podporou GPS) v mapových podkladech,
- zobrazení a tisk výpisů obchůzek podle přednastavených detailních a uživatelem definovaných filtrů,
- automatické odesílání e-mailových zpráv při navolených událostech,
- automatické zasílaní SMS při navolených událostech,
- informační text a banner upozorňující na stav systému, aktualizace, reklamní akce,
- automatický upgrade a archivace dat,
- integrované menu technické podpory.

On-line pochůzkový systém

Princip použití je v tom, že strážný obchází hlídanou lokalitu a čtečku (mobilní telefon) přikládá postupně k bezkontaktním čipům na kontrolovaných místech. Jednotlivé záznamy (přečtené čipy) jsou přes datové spojení okamžitě odesílány do databáze na serveru a jsou tak v reálném čase k dispozici dispečerovi, bezpečnostnímu manažerovi nebo zákazníkovi. Systém má mnoho nastavení a nabízí velkou řadu funkcionalit, které staví pochůzkovou činnost a její vyhodnocení na vyšší úroveň.

Hlavní funkce systému:[12]

1) strážný má možnost přihlásit se výběrem svého jména na čtečce a potvrzením PIN,
2) přiložením čtečky k prvnímu kontrolnímu bodu se spustí systém pro plánovanou pochůzku,
3) umožňuje nastavení různých typů pochůzek:

a) striktní – je stanoven čas mezi jednotlivými body, které se procházejí v přesně stanoveném pořadí,

b) libovolná – je stanoven pouze celkový čas pochůzky a kontrolní body bez ohledu na jejich pořadí,

[12] http://www.onlinepatrol.pl/cz/touchguard/simphony/

c) otevřená – není stanoven žádný čas, kontrolní body mohou být načteny v jakémkoliv pořadí i vícenásobně,

4) umožňuje zadat k jednotlivým kontrolovaným místům různé úkoly (například „kontrola oken"), přičemž je okamžitě vidět, zda a kdy byly úkoly splněny,

5) sleduje a vyhodnocuje přednastavené minimální a maximální časy v rámci pochůzek,

6) automaticky vyhodnocuje pochůzky v reálném čase a rozesílá hlášky o chybách v reálném čase,

7) v případě překročení času mezi dvěma body umožňuje automatickou kontrolu strážného, popřípadě možnost vyvolání alarmu (například v případě napadení strážného),

8) v případě plánovaného spouštění pochůzek lze trasu zvolit automaticky náhodným výběrem a přidělit ji strážnému; ten tak do poslední chvíle neví, kterou trasu půjde; tato možnost zvyšuje jeho osobní bezpečnost oproti možným rizikům při pravidelně opakovaných trasách pochůzek, které pachatel může vysledovat,

9) v případě nebezpečí je umožňuje aktivovat nouzové tlačítko na čtečce a přivolat pomoc.

7.9 Trezorové hospodářství

Milan Říha, Ladislav Sieger, Pavel Pikola

Ačkoliv obvykle není význam slova trezor a sejf rozlišován, je možno najít v sortimentu prodejců ochranných schránek rozdíl ve značení. Rozdíl je patrný z původu slov. Sejf pochází z anglického „saveů (chránit) a je primárně určen k ochraně uložených předmětů před zničením (vodou, teplem, ohněm, magnetickým polem apod.). Typický sejf je tedy dvouplášťová schránka s vnitřkem s izolací například z čedičové vaty. Trezor má původ v anglickém „treasure" (poklad) a je rovněž určen k ochraně svého obsahu, ale spíše před zloději. Typický trezor mívá schránku z tvrdé pancéřové oceli, železobetonu apod.

Bezpečnostní třídy trezorů

Základním kritériem pro hodnocení trezorů je jejich bezpečnost. Bezpečnost trezoru je odstupňována podle bezpečnostní třídy, do které se trezor zařazuje

podle dvou norem, české normy ČSN 916012 a evropské normy EN 1143-1. Norma EN 1143-1 upravuje bezpečnost trezorů v těch případech, kdy jsou kladeny vyšší požadavky na bezpečnost trezorů. Podle této normy se rozlišuje sedm bezpečnostní tříd (označení 0 až VI). Základní stupeň bezpečnosti trezorů upravuje norma ČSN 916012, která rozlišuje celkem tři stupně bezpečnosti.

Bezpečnostní třídy trezorů podle normy EN 1143-1

O tom, jak jsou trezory do příslušné kategorie zařazeny, informuje zájemce štítek na vnitřní straně dveří, který je pevně připevněn zpravidla nýtováním. Atesty o zařazení trezoru do bezpečnostní třídy vystavují certifikované zkušebny, které prošly certifikačním procesem a mají odpovídající znalosti a dovednosti. Klasifikace trezorů se shoduje v celé Evropské unii. Při klasifikaci trezorů provádějí zkušebny zkoušky v podobě násilného otevření trezoru.

Pro hodnocení trezoru se zohledňují použité nástroje a čas. Hodnocení trezoru se vyjadřuje jako hodnota odporu vyjádřené v jednotkách odporu RU (resistance unit). Čím je vyšší počet RU, tím vyšší je odpor a ochrana trezoru proti vloupání. Trezory jsou vždy klasifikovány podle nejnižšího změřeného odporu. Prolomení ochrany trezoru má podobu buď ručního otevření, potom se jedná o tzv. částečný průlom, nebo vylomení dveří, tedy tzv. plný průlom. Výsledky testů se následně převedou do hodnoty RU. Pro lepší orientaci v klasifikaci bezpečnostních tříd uvádíme orientační úložné částky v Kč. Pro zjištění příslušné finanční úložné částky je však vždy nutná konzultace s příslušnou pojišťovnou. Aby byly splněny požadavky bezpečnosti a zařazení trezoru do dané třídy, je nutno dodržet řádné ukotvení trezoru ve zdi či v podlaze nebo zazdění stěnových trezorů, které je vždy uvedeno v přiloženém návodu.

Bezpečnostní třídy sejfů

Sejfy jsou vlastně bezpečnostní schránky. Jsou rozděleny do dvou kategorií – zatříděná a nezatříděná ochrana:

1) VDMA-A – doporučená úložná částka do 20 000 Kč,

2) VDMA-B – doporučená úložná částka do 100 000 Kč.

Zabezpečení zbraní a střeliva

Dle nařízení vlády č. 338/2002 Sb., ve znění pozdějších předpisů (347/2003

Sb.), o technických požadavcích pro zabezpečení přechovávaných zbraní nebo střeliva, se za techniky způsobilé pro účely zabezpečení uschovávaných, uložených nebo uskladněných zbraní považují:

1) uzamykatelná ocelová schránka nebo uzamykatelná ocelová skříň, které splňují požadavky odolnosti proti vloupání 15 odporových jednotek (RU 15 – bezpečnostní třídy Z2) podle České technické normy ČSN EN 1143-1 a jsou vybaveny zámkem s vysokou bezpečností zařazeným do třídy A podle České technické normy ČSN EN 1300;

2) uzamykatelný skříňový trezor, který splňuje požadavky pro klasifikaci skříňových trezorů bezpečnostní třídy I podle České technické normy ČSN EN 1143-1;

3) uzamčená místnost nebo samostatný objekt (dále jen „zvláštní objekt") – zvláštní objekt je vybaven trezorovými dveřmi, které splňují požadavky pro kvalifikaci trezorových dveří a komorových trezorů bezpečnostní třídy I podle České technické normy ČSN EN 1143-1, nebo celoocelovými dveřmi, které splňují tytéž požadavky.

Ochrana nosičů dat

Ohnivzdorné trezory pro počítačové nosiče dat jsou určeny k bezpečné archivaci všech typů datových médií. Testovaná odolnost před účinky požáru o teplotě 1100 °C je zaručena po dobu 60 nebo 120 minut. Datové nosiče jsou extrémně citlivé na teplo, kterým mohou být poškozeny, v důsledku čehož by mohly být cenné informace navždy ztraceny. K tomu může dojít již při teplotě 55 °C. Běžné trezory a kovové skříně přitom nejsou schopny ochranu dat zajistit. Je-li potřeba data bezpečně archivovat a zároveň je i chránit před zničením ohněm, vlhkostí či zmagnetizováním, jsou pro vás ohnivzdorné trezory jediným řešením. Ohnivzdorné trezory jsou testovány a certifikovány podle celoevropsky platné normy EN 1047-1. Diskety, streamry, DAT kazety, videokazety, optické disky jsou schopny odolat maximální teplotě 55 °C, CD-ROM a DVD vydrží cca 70 °C a papír maximálně teplotu 175 °C (uvažujeme-li max. vlhkost vzduchu cca 85 %). Někdy může mít zákazník požadavek též na pádovou odolnost.

Způsoby instalace trezorů a sejfů

- Kotvení trezorů a sejfů

Provádí se z důvodu, aby nedošlo k odnesení celého trezoru a následně k jeho násilnému otevření; trezory a sejfy tedy kotvíme v zájmu bezpečného uložení cenností; z tohoto důvodu dělíme kotvení podle toho, jak daný trezor nebo

sejf chceme ukotvit – a to do stěny nebo do podlahy; pro kotvení je nutné přihlédnout k materiálu zdiva, do kterého chceme trezor nebo sejf ukotvit:

1) železobeton, beton, kámen – mechanické kotvení rámovou kotvou s křížovou hlavou, šroub M10;

2) zdivo z plných cihel, zdivo z děrovaných cihel, porotherm – mechanické kotvení univerzální hmoždinkou se šestihrannou hlavou;

3) zdivo z plných cihel, zdivo z děrovaných cihel, zdivo z porothermu – chemické kotvení pomocí kotvy určené pro tento druh materiálu.

▪ Zazdívání trezorů a sejfů

Stěnové trezory mají být zazděny do otvoru ve zdi nebo v podlaze, kdy musí být dodržena nejméně 100mm vrstva betonu o pevnosti minimálně 40 MPa (v tlaku kolem trezoru mimo čelní strany). Při umístění trezoru nebo sejfu do venkovní stěny se doporučuje tento ze zadní strany tepelně izolovat – zabrání se tím vysrážení vody uvnitř trezoru nebo sejfu při větších tepelných rozdílech uvnitř a vně budovy. Po dobu zrání betonu se doporučuje nechat dveře trezoru pootevřeny.

Komorové trezory

Komorový trezor je vhodný k dlouhodobému zabezpečení pokladní hotovosti, zlata, drahých kamenů, cenin, mincí, důležitých dokumentů, kreditních karet, šeků a valut. Komorový trezor se projektuje dle potřeb uživatele, je vhodný zejména pro banky, finanční instituce, ale i soukromé objekty. Modulové řešení komorového trezoru je moderní konstrukce, která zvyšuje jeho odolnost proti napadení a usnadňuje jeho instalaci i případnou demontáž. Komorový trezor je chráněn proti použití nejmodernějšího diamantového nářadí. Moduly jsou v provedení podlahové, stěnové, stropní, ventilační, s průchodkami pro přívod elektrické energie, počítačovou síť, průmyslové kamery a PZTS, modul nouzového východu je dodáván pouze v nejvyšší bezpečnostní třídě XI. Dveře komorového trezoru jsou vybaveny zámkovým systémem mechanickým nebo elektronickým s možností auditu. Dveře mohou být dle konkrétní potřeby uživatele doplněny vnitřní brankou v plném nebo proskleném provedení, vnitřní mříží, předtrezořím – předsíní s trezorovými dveřmi. Trezorové dveře komorového trezoru jsou dodávány i samostatně, jsou vhodné pro komorové trezory modulové i monolitické. Komorové trezory upravuje ČSN 91 6010 – Úschovné objekty – Zkušební metody a klasifikace odolnosti proti vloupání – Skříňové a komorové trezory.

Komorový trezor je dle ČSN EN 1143-1 definován jako úschovný objekt, který chrání obsah proti vloupání a který v zavřeném stavu má všechny délky vnitřních stran větší než 1 m. Skříňový trezor je definován stejně, jen s tím rozdílem, že má délku alespoň jedné vnitřní strany menší nebo rovnu 1 m.

Atypické druhy trezorů

▪ Trezor s vhozem

Trezor s vhozem se vyznačuje možností rychlého uložení peněz, cenností, dopisů bez potřeby otevření samotného trezoru. Pokladník pouze otevře zásuvku v horní části trezoru, vloží do ní hotovost a zásuvku opět uzavře. Při uzavírání zásuvky se začne otevírat propadliště v jejím dně, což zapříčiní propadnutí vložené hotovosti do vlastní trezorové části, kterou je možno otevřít pouze samostatným klíčem. Pokud pokladník klíč k vlastnímu trezoru nemá a navíc je na tuto skutečnost případný pachatel upozorněn např. nápisem „OBSLUHA NEMÁ OD TREZORU KLÍČ", odchází zpravidla s nepořízenou, nechce-li ovšem riskovat ztrátu značného času potřebného k násilnému vniknutí do trezoru. Trezor je následně vyprázdněn např. bezpečnostní službou, která zajišťuje bezpečný převod hotovosti do banky. Zvýšení bezpečnosti s využitím trezoru s vhozem je možné např. na benzinových čerpacích stanicích nebo v obchodech, které pracují s vyššími denními tržbami apod.

▪ Autotrezor

Trezor do auta je určen pro snadnou montáž do prostoru rezervního kola automobilu, nebo u nových vozů do prostoru, který byl pro rezervu určen. Trezor se snadno upevňuje bez dalších nároků na vrtání a upevňování a svým umístěním poskytuje kvalitní zabezpečení. Trezor se dodává s variantou zámku na klíč.

▪ Trezory s časovým zámkem

Tento typ trezorů může být otevřen nebo vyzvednut pouze v době předem naprogramované (např. doba příjezdu bezpečnostní převozní služby). Viditelně umístěná výstraha o instalaci tohoto typu trezoru případného lupiče předem odradí a tím odvrátí nebezpečí přepadení obsluhy. Své uplatnění nachází tento typ trezoru nachází zejména v bankách, na poštách a na všech místech, kde hrozí přepadení pokladny, v níž se nachází značná finanční hotovost.

Použitá literatura

ŘÍHA, Milan; SIEGER; Ladislav, PIKOLA, Pavel: *Bezpečnostní systémy III*. Námořní akademie České republiky. Praha 2011. ISBN 978-80-87103-35-7. Str. 14–20.

Aby byly splněny požadavky bezpečnosti a zařazení trezoru do dané třídy je nutné dodržet řádné ukotvení trezoru ve zdi či v podlaze nebo zazdění stěnových trezorů, které je vždy uvedeno v přiloženém návodu.

Bezpečnostní třída	Nejnižší počet zámků	Nejnižší požadovaná třída bezpečnost. zámku	Orientační úložná částka	Odporové jednotky
0	1	A	100.000,- Kč	RU (30/30)
I	1	A	300.000,- Kč	RU (30/50)
II	1	A	500.000,- Kč	RU (50/80)
III	1	B	5.000.000,- Kč	RU (80/120)
IV	2	B	6.000.000,- Kč	RU (120/180)
V	2	B	16.000.000,- Kč	RU (180/270)
VI	2	C	30.000.000,- Kč	RU (270/400)

Trezory rozdělené podle zákona o ochraně utajovaných informací a vyhlášky NBÚ do stupňů utajení

stupeň V	pro utajované informace ve stupni Vyhrazené	třída 0
stupeň D	pro utajované informace ve stupni Důvěrné	třída 0
stupeň T	pro utajované informace ve stupni Tajné	třída I
stupeň PT	pro utajované informace ve stupni Přísně tajné	třída II

Trezory rozdělené podle zákona o ochraně utajovaných informací a vyhlášky NBÚ do stupňů utajení

Bezpečnostní třída	Nejnižší počet zámků	Nejnižší požadovaná třída bezpečnostního zámku	Orientační úložná částka	Odporové jednotky
Z1	1	A	0,- Kč	RU (10/10)
Z2	1	A	30.000,- Kč	RU (15/20)
Z3	1	A	50.000,- Kč	RU (20/25)

8. INTEGRACE BEZPEČNOSTNÍCH TECHNOLOGIÍ

Jaromír Kyncl

V této stati pomineme výčet a popis principu fungování sofistikovaných komplexních systémů pro evidenci prvků a řešení úkolů evropských, národních, krajských a dalších institucí a resortů krizového řízení, které by měly obsahovat nejvyspělejší softwarové nástroje pro analytické, plánovací, řídicí a komunikační úlohy. Tyto systémy samozřejmě akceptují nejmodernější přístupy k integraci bezpečnostních technologií, systémů a subsystémů, metodologicky sjednocují postupy při plánování krizové připravenosti a umožňují sdílet operativní informace při reakci na krize a mimořádné události. Současně tak přispívají k minimalizaci škodlivých následků. Pro naše potřeby jsou důležité integrace bezpečnostních technologií na objektech, ve kterých se pohybuje velké množství osob a v nichž je možno usuzovat na zvýšená bezpečnostní rizika včetně rizik páchání protiprávního jednání.

Hlavní přínos integrace bezpečnostních systémů spočívá v efektivním automatickém řízení budov, provázání systémů při řešení bezpečnostních incidentů, havarijních a evakuačních postupů v budovách i celých areálech. Nespornou výhodou integrace je snadné a intuitivní ovládání v jednotném grafickém prostředí, celkový přehled a grafický dohled nad stavem monitorovaných situací, jednotné zpracování dat včetně předávání výsledků a přehledné zobrazení sledovaných stavů v reálném čase.

Spojení různých bezpečnostních technologií – tzn. systémů CCTV, kontrolních bodů obchůzkových systémů, detektorů narušení, požárních hlásičů, prvků přístupových, docházkových, komunikačních i jiných zařízení – to vše slouží ke snadnějšímu a efektivnějšímu zajištění bezpečnosti jednotlivých budov i celých areálů. Z více samostatných infrastruktur se dají tvořit celky se snadným ovládáním a jednoduchou správou a s možností propojení s dalšími informačními systémy střeženého podniku. Vzniká tak ucelené řešení, jehož podoba odpovídá potřebám a možnostem organizace.