Současné směry oblasti v zajištění fyzické bezpečnosti objektů a areálů státní správy

Current Directions of the Area in Ensuring the Physical Security of State Administration Buildings and Premises

MICHAL STRNAD¹
VLADIMÍR OLIBERIUS²

Abstrakt

Příspěvek se zabývá současnými směry při zajištění objektů a areálu státní správy. Autoři se zabývají možností vyhodnocování signalizace z různých typů bezpečnostních a detekčních systémů. Velmi krátce se věnují přínosu nadstavbových bezpečnostních systémů při vyhodnocování nových technologií v rámci jednotných bezpečnostních systémů. V druhé části je věnována pozornost vstupním klíčovým systémům. Jsou zde popsány klady a zápory, včetně upozornění na jeden z nejnovějších klíčových vstupních systémů, zejména s ohledem na jeho přínos pro fyzickou bezpečnost objektů a areálů.

Klíčová slova

fyzická bezpečnost, objektová ochrana, bezpečnost objektů a areálů státní správy, jednotný bezpečnostní systém, bezpečnostní nadstavbový systém, integrované poplachové systémy, vstupní klíčové systémy, bezpečnostní požadavky na klíčové systémy

Abstract

The paper deals with current trends in securing objects and premises of state administration. Authors deal with possibilities of signaling evaluation from various types of security and detection systems. They deal very briefly with the benefits of additional security systems in the evaluation of new technologies within the framework of uniform security systems. The second part is devoted to the key input systems. The pros and cons are described here, including notifications of one of the latest key entry systems, especially with regard to its contribution to the physical security of buildings and sites.

Key words

physical security, object protection, security of public administration buildings and premises, unified security system, safety superstructure system, integrated alarm systems, entry key systems, security requirements for key system

DOI

<http://dx.doi.org/10.37355/fvpk-2021/1-07>

¹ Mgr. Michal Strnad, Ministerstvo financí, odbor bezpečnosti

² Mgr. Vladimír Oliberius, Ph.D., znalec v oborech fyzické bezpečnosti

Úvod

Objekty a areály stání správy jsou mnohdy řazeny pod tzv. měkké cíle, tedy mělo by se dle této terminologie jednat o místa s vysokou koncentrací osob a s nízkou mírou zabezpečení. Reálně tomu tak však není, a ani být nemůže. Zejména stav fyzické a objektové bezpečnosti v případě objektů a areálů ministerstev zcela nepochybně této definici nevyhovuje. Právě naopak, jedná se o místa, kde se k fyzické a objektové bezpečnosti přistupuje velmi uváženě, rizika nejsou podceňována a je snaha postupovat při zajištění bezpečnosti těchto objektů i moderními metodami. V uvedeném příspěvku je krátce načrtnuto, jakým směrem by se mělo zajištění fyzické a objektové bezpečnosti dále vyvíjet. Zcela samostatně je věnována pozornost vstupním klíčovým systémům, jejichž důležitost pro naplnění bezpečnostních cílů je stále podceňována.

1 Fyzická bezpečnost

Pod pojmem fyzická bezpečnost rozumíme soubor opatření k zajištění požadovaného stavu bezpečnosti nebo bezpečí. V české terminologii se používají oba pojmy. Význam nebo spíše způsob použití pojmů je nejlépe odvoditelný od širšího kontextu. Jedná se buď o stav, který je obecněji nazýván bezpečnost, a pod pojmem zabezpečení rozumíme soubor opatření.

Systémy a opatření fyzické bezpečnosti slouží k ochraně hmotného a nehmotného majetku a k zajištění bezpečnosti osob, slouží též k eliminaci rizik spojených s činností konkrétního subjektu. Zajištění fyzické bezpečnosti je chápáno v několika vrstvách. V první řadě se jedná o interní směrnice příslušného subjektu, kdy na vrcholu interních předpisů by měl být dokument označený jako *Bezpečnostní politika*. Z tohoto dokumentu pak vychází další nezbytné interní předpisy zejména *Ochrana majetku a ostraha majetku státu*, *Výkon ostrahy objektů*, *Analýza bezpečnostních rizik* a další dokumenty. Všechny dokumenty musí tvořit ucelený a logicky na sebe navazující celek. Formální stránka, tedy interní předpisy, musí popsat cíle fyzické bezpečnosti.

Cíl fyzické bezpečnosti

- odradit nebo odstrašit možného pachatele (útočníka),³
- zabránit vzniku nežádoucího stavu⁴ (nemusí jít nutně o kriminální delikt),
- znesnadnit provedení, ztížit provedení a prodloužit dobu pro spáchání skutku,
- opatřením(-i) vytvořit podmínky vedoucí ke vzniku různých typů stop,
- vytvořit podmínky pro možnou identifikaci (nejenom osob),
- zajistit možnost řešit skutek (incident) s konkrétní osobou v rámci pracovněprávního vztahu, správního řízení apod., ryze kriminální delikty předat policii.

³ Neumožnit realizovat motivaci.

⁴ Viz objektivní odpovědnost.

Systém fyzické bezpečnosti

Systém fyzické bezpečnosti představuje soubor opatření, jejichž účelem je zajištění požadovaného stupně (stavu) bezpečnosti (bezpečí). Vytvoření účinného systému fyzické bezpečnosti předpokládá logický postup při realizaci, a to zároveň při dodržení určitých zásad, jako je komplexnost, víceúrovňovost, automatizace, možnost propojení technologií s režimovými opatřeními, odolnost opatření a systémů.

Systém fyzické bezpečnosti je tvořen režimovými opatřeními, technickými prostředky a fyzickou ostrahou. Osobně jsem přesvědčen o tom, že nedílnou součástí fyzické bezpečnosti jsou opatření právní, za která považujeme nejen zákony (z nichž odvozujeme část rizik), normy, ale nepochybně jde i o interní akty subjektů bez ohledu, zde jde o povinné (např. osobní údaje) či nepovinné akty.

Objektová ochrana

Objektová ochrana je součástí fyzické ochrany a většinou se skládá z prvků perimetrické a plášťové ochrany, případně z některého ze systému nebo opatření v oblasti kontroly vstupu.

Rizika a stanovení jejich závažnosti

Základní pomůckou pro identifikaci rizik v organizaci je nauka zabývající se řízením rizik v organizaci. Jedná se o hraniční obor bezpečnosti a managementu. Závažnost rizik se stanovuje podle dvou základních kritérií:

- a) četnost výskytu,
- b) závažnosti následku.

Dohledové vyhodnocovací centrum a integrované systémy

V době možností využití různých moderních technologií má pracoviště dohledového centra nejen svoje opodstatnění, ale v současné době je základem fyzické bezpečnosti objektů a areálů státní správy. Na pracoviště dohledového vyhodnocovacího centra jsou svedeny různé typy poplachových i nepoplachových signalizací. Obecně jsou označovány jako *integrované poplachové systémy*. Jedná se o takové systémy, které mají jedno nebo více společných zařízení, z nichž alespoň jedno je zařízení, které patří k některému z typů poplachové aplikace. Zařízení by mělo vyhovovat příslušné normě.⁵ Mezi bezpečnostními poplachovými systémy patří systémy určené k ochraně života, majetku nebo prostředí:

- poplachové zabezpečovací a tísňové systémy,
- systémy přivolání pomoci,
- uzavřené kamerové systémy využívané pro účely zabezpečení nebo dohledu,
- systémy kontroly vstupu určené pro použití v bezpečnostních aplikacích,
- elektrická požární signalizace,
- poplachové systémy vlivu prostředí a poplachové systémy výtahů,
- klíčového hospodářství, minimálně na úrovni evidence držitelů.

5 ČSN CLC/TS 50398 (334597) – Poplachové systémy – Kombinované a integrované systémy – Všeobecné požadavky.

Tyto systémy mohou být integrovány různě navzájem a dle potřeby mohou být doplněny o nepoplachové systémy, kterými jsou zejména:

- osvětlení, vytápění,
- klimatizace, ventilace,
- detekce zásob technických plynů,
- detekce výtahů,
- správa budov, řízení energetických systémů,
- zavlažování, vysoušení,
- další různé aplikace.

Právě integrace různých systémů do dohledového centra přináší mnohá pozitiva. Hlavní výhodou integrace systémů je především zvýšení účinnosti jednotlivých propojených systémů, zvýšení přehledu o situaci v objektu, v systému budov, v areálu, a tím je zvýšení standardu fyzické bezpečnosti a zároveň přináší snížení počtu osob vykonávajících dohled, ostrahu, tedy snížení dlouhodobých nákladů, v případě vzniku bezpečnostního incidentu poskytuje důležité informace.

Integrace je prováděna vždy ve dvou úrovních, jedna úroveň je v oblasti hardwarových řešení (HW) a druhá je v oblasti softwarových řešení (SW). HW oblast řeší vzájemné propojení systémů pomocí vstupů a výstupů a dále řeší technické parametry systémů, kdy jsou mnohdy základní bezpečnostní funkce rozšířeny o specifické moduly (prvky). Oblast SW řeší propojení aplikací prostřednictvím komunikační sběrnice. Správa, řízení a vizualizace je zajišťována SW produkty na různých typech zařízení.

Druhá rovina (*systémy pro správu fyzického zabezpečení*) je označována taktéž pojmem bezpečnostní nadstavbové systémy a je v podstatě komplexnějším řešením roviny první. Jde o souhrn HW a SW prostředků, které integrují nezávislé bezpečnostní aplikace a zařízení do jednoho funkčního celku a ovládají je pomocí jednotného (komplexního) uživatelského rozhraní. Aplikace detekuje, shromažďuje a vyhodnocuje události ze zapojených různorodých bezpečnostních zařízení (systémů) a informačních systémů. Mimo běžné funkce může přinášet i informační management a situační analýzu.

Tyto systémy pomáhají snížit bezpečnostní a provozní rizika, neboť zachycují, vyhodnocují, porovnávají korektní informace z mnoha zdrojů, čímž poskytují komplexní situační přehled o situaci v chráněném prostředí. Výrazně zlepšují dobu reakce na rizika, umožňují zlepšit prevenci a fyzickou bezpečnost. Základními výhodami bezpečnostních nadstavbových systémů jsou v obecné rovině:

- zlepšený globální přehled o reálné situaci v objektu, areálu, ale i v několika vzdálených objektech a areálech,
- rychlejší reakce obsluhy nebo bezpečnostní služby na událost,
- efektivnější využívání zdrojů, včetně personálních,
- snížení chybných (planých) poplachů,
- eliminace chyb lidského faktoru,
- jednotné řešení.

Pracoviště dohledové centra jakožto součást fyzické bezpečnosti musí samo o sobě splňovat některá kritéria bezpečnosti. Bezpečnost dohledového centra je velmi důležitý

parametr. Bez hladkého a bezpečného chodu tohoto pracoviště by nešla zajistit fyzická a objektová bezpečnost. Samotné dohledové centrum by tedy mělo umět reagovat či být dostatečně odolné vůči níže uvedeným rizikům:

- *útok zvenčí (narušitel)* – budova nebo oblast umístění dohledového centra by měla být vybavena poplachovým systémem, včetně výstrahy pro personál dohledového centra o narušení nebo o pokusu narušení chráněného prostoru,
- *požár* – budova, kde je umístěno dohledové centrum, by měla být vybavena elektrickou požární signalizací,
- *vchod a východ* – měla by být instalována akustická nebo optická signalizace upozorňující pracovníky dohledového centra o tom, že jsou nezajištěné přístupové dveře, indikace otevření nouzového východu apod., vstupy, výstupy a nouzové východy musí splňovat bezpečnostní požadavky na odolnost dveří, rámtů, vložek, kování, a to jak u elektromechanických, tak u mechanických zámkových systémů atd.,
- *plyn* – je vhodné mít vybavené pracoviště minimálně detekcí oxidu uhelnatého, která bude reagovat na zvýšenou hladinu plynu ještě dříve, než dojde ke stavu nasycení vyžadujícímu evakuaci,
- *komunikace* – veškerá kabelová a bezdrátová komunikační zařízení uvnitř objektu sloužící k přenosu detekovaných informací (poplachové i nepoplachové, videopřenos) do nebo z dohledového centra musí být chráněna,
- *tíseň (přepadení)* – instalace tíšňového systému, včetně tíšňových hlásičů (PANIK), umístění v blízkosti vstupních dveří, nouzového východu, komunikačních okének apod.,
- *monitorování bezpečnosti personálu, např. CCTV* – měl by být instalován kamerový systém, který umožní personálu dohledového centra identifikovat oprávněné osoby před vstupem do vnitřní části centra, kamera má být umístěna na úrovni vstupu,
- *signalizace elektronických ochranných systémů* – signály zabezpečení dohledového centra musí být přenášeny do jiného dohledového centra a jejich přenos musí odpovídat určitým technickým parametrům, jako je doba přenosu, dostupnosti informace apod.

Vždy platí, že jakékoli kabelové připojení do dohledového centra nesmí být vyvedeno ze země dříve než za hlavní domovní zdí objektu, v němž se nachází dohledové centrum nebo je odděleně umístěna vyhodnocovací technologie.

2 Vstupní klíčové systémy

Klíčové systémy jsou dlouhodobě a trvale podceňované prvky fyzické a objektové bezpečnosti. Klíčový systém neplní pouze funkci jakéhosi oddělení prostoru mezi vnějším a vnitřním prostředím, nebo mezi společnými chodbami a prostředím kanceláří. Klíč a celý klíčový systém, včetně zámků, krytů zámků, konstrukce dveří, zárubní, pantů dveří apod. dnes neplní pouze funkci při ochraně majetku. Klíč nesmí být volně kopírovatelný. V současné době je možno tvrdit, že právě ochrana majetku státu, úřadu nebo zaměstnanců není tím hlavním rizikem, proti kterému má být kvalitní vstupní klíčový systém určen. V moderním

pojetí slouží vstupní klíčové systémy k ochraně osobních údajů, k ochraně utajovaných nebo důvěrných informací, má sloužit např. k průkaznosti vstupu do režimových oblastí. Vstupní klíčový systém musí být buď součástí komplexu bezpečnostních opatření objektu, nebo areálu, měl by tedy být pevnou součástí jednotného bezpečnostního systému, nikoli jeho slabinou. V ideálním případě by měl být schopen na definovaných místech předávat informace do nadstavbového vyhodnocovacího systému.

Bezpečnostní požadavky se tedy promítají do požadavků technických a funkčních. Technické a funkční požadavky klíčového systému by tedy měly plnit níže uvedené požadavky:

- možnost zpětné auditovatelnosti přístupů,
- jednoznačnost jednoznačné identifikace,
- nemožnost pořizování kopií klíčů, čímž by docházelo ke ztrátě kontroly nad režimem přístupu,
- nastavení osobní odpovědnosti uživatelů klíčového systému,
- možnost nastavení striktních režimových pravidel přístupu na konkrétní místa.

Z tohoto nástinu základních požadavků na klíčové systémy je zřejmé, že klíč nemůže být v jednotném bezpečnostním systému brán jako jeden prvek. Je nutno tedy hovořit o vstupním systému. Vstupní klíčový systém pak musí splňovat požadavky na systém, které v současné době jsou tyto:

- systém kombinující mechanické a elektronické prvky „zámkové vložky a klíče“ – umožňující řízení přístupových práv do jednotlivých prostor bez nutnosti provedení stavebních úprav a instalace kabeláže,
- certifikace systému nejméně pro 3. bezpečnostní třídu⁶ (včetně odpovídající certifikace NBÚ),
- systém nezmění vzhled dveřního křídla z důvodu památkové ochrany budov,
- správa přístupových práv jednotlivých klíčů je vzdálená bez nutnosti zásahu u vložek pomocí obslužného SW a nástěnných programovacích jednotek připojených do sítě klienta,
- správa přidělování oprávnění může být rozdělena pro jednotlivé uživatele objektu, to znamená, že pokud má objekt např. 8 pater, pak jedna konkrétní osoba dostane oprávnění přidělovat kódy ke dveřím ve 3. a 5. patře, druhá konkrétní osoba v přízemí a 4. patře a další osoba ke zbytku objektu,
- klíčový systém je koncepčně řešen takovým způsobem, aby byl do budoucna rozšiřitelný na více objektů, jejichž správa (včetně přidělování oprávnění ke vstupu) bude ovládána dálkově, a rovněž bude umožňovat tvorbu tzv. lokálních správců, kteří budou mít programovací pravomoc pouze ke svěřené části,
- zabezpečení přístupu do obslužného SW pomocí HW/SW klíče/kódu,
- elektronická evidence všech vyrobených a vydaných klíčů (databáze klíčového hospodářství); přehled o stavu přístupových práv jednotlivých osob v rámci SGHK; generování/export datových sestav s údaji z klíčového hospodářství pro další zpracování (např. ve formátu .csv/.xls),

6 Bezpečnostní třída 3. Dle ČSN EN 1627. Systémy jakými jsou kartové vstupní systémy typu – čtečka karet/otisk prstu/PIN/klávesnice nebo kování se čtečkou karet nebo vložky se čtečkou karet v současné době požadavky na bezpečnostní třídu 3 nesplňují. Důvodem je slabá konstrukční odolnost.

- tisk protokolu o výdeji klíče do objednatelům dodané el. šablony (formulář),
- určování přístupových práv pomocí časových údajů (**od** datum/čas – **do** datum/čas),
- vyčítání historie přístupů z klíčů automaticky (časové údaje a identifikace klíče),
- změna přístupových práv dálková automatická,
- systém musí umožnit rozšíření na další objekty a dálkové ovládání těchto objektů pomocí obslužného softwaru a nástěnných programovacích terminálů.

3 Mechatronické klíčové systémy

V současné době splňuje výše uvedené požadavky technologie mechatronických zámků. Zcela samozřejmě se jedná o patentovanou technologii CLIQ. Uvedená technologie rozšiřuje klasické cylindrické vložky o fyzicky odolnou elektronickou blokovací lištu. Vstupní klíčový systém je založen na napájení z baterie, která je umístěna pouze v uživatelském klíči. Není tedy nutné složitě protahovat kabeláž a jakkoliv zasahovat do omítek a dveřních křídel. Zámek lze použít na všech bodech, kde již byla cylindrická vložka instalována. Výhodou systému je rychlost a snadnost montáže, včetně zachování původního vzhledu dveřních křídel. Ke dveřím není nutno přivádět kabeláž. Vložka zámku je odolná, vyrobená z mosazi nebo z titanu. Tento zámkový systém je schválen i pro ochranu utajovaných informací⁷ do stupně „tajné“. Výhodou mechatronického zámkového systému je možnost zablokování ztracených klíčů, možnost časové volby přístupu, změny práv uživatelů a historie přístupů.

Velmi podstatnou okolností je i ta skutečnost, že na trhu nejsou nelegální výrobci klíčových profilů tohoto systému. To je ze dvou důvodů. V první řadě je „řezačka“ profilů relativně drahá a za druhé, samotný vyřezaný profil nelze použít. To je v systému zajištění fyzické bezpečnosti velice důležitá okolnost. Nemůže se stát, že by neexistovala kontrola přístupů, že by neexistovala kontrola nad tím, jaká osoba má v držení funkční klíč.

Součástí systému je zařízení provádějící správu klíčového systému, a to v řádu tisíců uživatelů. Na tomto zařízení určeném pro správu se provádí kódování klíčů a zámků, správce systému (uživatel) může měnit přístupová oprávnění, přístupová oprávnění mohou být časově omezena a v případě prolomení bezpečnosti mohou být oprávnění smazána a klíč tak vyřazen z možnosti použití. Jednotliví uživatelé si na zařízení automatizovaně mění přístupové kódy v určených časových intervalech. Uvedené zařízení může z klíčů a těl zámků načíst historii přístupů. Ve variantě provedení „remote“ pak dochází vždy při obnově kódování k automatickému stažení údajů z klíčů.

Bezpečnost a výhody – shrnutí

- Kombinace mechanického a elektronického zabezpečení,
- kryptomerické kódování elektroniky klíčů,
- nemožnost výroby neoprávněné kopie klíčů,
- okamžitá změna přístupových práv (např. při ztrátě klíče),

⁷ Ve smyslu zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti.

- akustická a vizuální signalizace přístupů elektronických klíčů,
- možnost zpětné auditovatelnosti historie přístupů z elektronických klíčů a vložek,
- jednoznačná správa klíčového hospodářství v rámci ovládacího SW,
- neomezené možnosti přístupových práv elektronických klíčů,
- možnost definování přístupových časů elektronických klíčů,
- změna přístupových práv bez dalších nákladů,
- možná výměna za jakoukoli cylindrickou vložku,
- nejsou náklady na slaboproudé instalace,
- lze použít i v památkově chráněných objektech.

Subjekt, který využívá uvedený systém klíčového hospodářství, však musí splňovat některé požadavky vycházející ze zásad zpracování osobních údajů a jejich ochrany. Hlavní právní normou je Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, případně další právní předpisy EU⁸ či členského státu.

Závěrečné shrnutí

Účelem tohoto článku je v rámci krátkého exkurzu do problematiky nastínit současné směry při zajišťování fyzické bezpečnosti objektů a areálů státu. Článek se věnuje fyzické a objektové bezpečnosti, z pohledu možnosti využití bezpečnostních technologií. Hlavním cílem je specifikovat výhody, jednotného, integrovaného poplachového systému v návaznosti na činnost dohledového centra. V příspěvku je upozorněno i na nutnost zajištění parametrů fyzické bezpečnosti samotného dohledového centra. V druhé části je pozornost věnována klíčovým systémům, které jsou doposud největší slabinou bezpečnostních systémů. Jsou zde specifikovány bezpečnostní požadavky na klíčové vstupní systémy. Na závěr je představen typ technologie klíčového systému, který požadavkům na bezpečnost v současné době vyhovuje nejvíce.

Použitá literatura

- 1) LUKÁŠ, Luděk a spol. *Bezpečnostní technologie, systémy a management*. Zlín: VerBum, 2015, 368 s. ISBN 978-80-87500-67-5.
- 2) TICHÝ, Milík. *Ovládání rizika, Analýza a management*. Praha: C. H. Beck, 2006, 396 s. ISBN 80-179-415-5.

Ostatní:

- 1) OLIBERIUS, Vladimír: znalecký posudek ev. č. 265/2018, soukromý archiv spoluautora.

8 Např. Směrnice 2016/680 (zpracování osobních údajů orgány činným v trestním řízení) nebo Směrnice 2016/681 (prevence a odhalování závažné trestné činnosti a stíhání teroristických trestných činů).

Právní předpisy a normy:

- 1) Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.
- 2) Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.
- 3) ČSN EN 1627 – Dveře, okna, lehké obvodové pláště, mříže a okenice – Odolnost proti vloupání – Požadavky a klasifikace.
- 4) ČSN CLC/TS 50398 (334597) – Kombinované a integrované systémy – Všeobecné požadavky.
- 5) ČSN EN 50518 ed. 2 – Dohledová a poplachová přijímací centra – Umístění a konstrukční požadavky.