Zabezpečení bankovního domu
Bank Building Security

Bc. Marie Opluštilová

Diplomová práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Marie OPLUŠTILOVÁ**
Osobní číslo:	**A10908**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Zabezpečení bankovního domu**

Zásady pro vypracování:

1. **Analýza současného stavu zabezpečení.**
2. **Bezpečnostní politika bankovního domu.**
3. **Vnější bezpečnostní rizika.**
4. **Ochrana přepážkovýh pracovišť.**
5. **Návrh na snížení bezpečnostních rizik**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **KINDL, Jiří. Projektování bezpečnostních systémů I. 2. vydání Zlín: Univerzita Tomáše Bati ve Zlíně, 2007. 134 s. ISBN 978-80-7318-554-1.**
2. **ČERNÝ, J., IVANKA, J. Systematizace bezpečnostního průmyslu I. 1. vydání Zlín: Univerzita Tomáše Bati ve Zlíně, 2005. 133 s. ISBN 80-7318-310-2.**
3. **JAŠEK, R. Informační a datová bezpečnost. 1. vydání Zlín:Univerzita Tomáše Bati, Academia centrum, 2006.140 s. ISNB 80-7318-456-7.**
4. **RAK, R., MATYÁŠ, V., ŘÍHA, Z., Biometrie a identita člověka ve forenzních a komerčních aplikacích. 1. vydání Praha: Grada Publishing, a.s., 2008, 664 s. ISNB 978-80-247-2365-5.**
5. **LUDVÍK, M., ŠTĚDROŇ, B., Teorie bezpečnosti počítačových sítí. 1. vydání. Praha:Computer media, 2008.99 s. ISBN 978-80-86686-35-6**

Vedoucí diplomové práce: **JUDr. Josef Čejka**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **24. února 2012**

Termín odevzdání diplomové práce: **15. května 2012**

Ve Zlíně dne 24. února 2012

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práce se zabývá zabezpečením bankovních domů, jejímž cílem je snížit bezpečnostní rizika na bankovních přepážkách a při výběrech hotovostí z bankomatů. Práce je rozdělena na teoretickou a praktickou část. V teoretické části jsou popsány formy současné ochrany majetku a osob a možnosti zabezpečení. V praktické části navrhuji bezpečnostní opatření na snížení bezpečnostních rizik

Klíčová slova: poplachové zabezpečovací systémy, mechanické zábranné systémy, bezpečnostní analýzy, informační bezpečnost

ABSTRACT

The thesis is focused on the Bank Building security where the goal is to reduce the security risks on the Bank cash desks and during the ATM cash withdrawal. Thesis is divided into a practical part and a theoretical part. In the theoretical part are described today forms of property and persons protection and security possibilities. In the practical part are suggested security measures for security risks reduction.

Keywords: alarm security systems, mechanical block systems, security analysis, security assessment, information security

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Předcházení rizikových situací vyžaduje věnovat zvýšenou pozornost fyzické bezpečnosti, režimovým opatřením a technickému vybavení. Pro bankovní domy jsou tato opatření nezbytná a platí o to víc, čím větší je riziko vniknutí a přepadení bankovního domu. Bankovní domy plní svou funkci uspokojování finančních potřeb klientů, provádění bezhotovostních plateb a s tím souvisí nutnost mít k dispozici hotovost na pobočkách finančních ústavů. Pro finanční ústavy představuje zabezpečení neustálý koloběh obměny technického vybavení, zavádění nových technických prvků a reagování na požadavky pojišťoven. Musí počítat s informovaností a technikou, která je dostupná i pachatelům. Pachatelé stále vymýšlejí způsoby jak se bez většího rizika dostat k finanční hotovosti. V mnoha případech již není vniknutí a přepadení pobočky vzhledem ke zvýšenému riziku dopadení pro pachatele atraktivní a vymýšlí stále nové podvody, jak finanční hotovosti získat. I bankovní domy snižují své pokladní limity, tak aby odcizená hotovost neodpovídala riziku, které musí pachatel podstoupit. Loupežné přepadení se řadí mezi nejzávažnější společenské zločiny, při kterých dochází k útoku na cizí majetek, kde může být narušena tělesná integrita oběti, vyvolaná násilím nebo pohrůžkou bezprostředního násilí.

V současné době pachatelům nahrává nepozornost klientů při výběrech hotovosti z bankomatů. Klienti většinou z neznalosti a neopatrnosti podceňují fakt, že by se mohli stát obětí podvodu při výběru z bankomatu. Bankomat berou jako nástroj, jak se dostat ke své hotovosti na účtu. Tohoto využívá pachatel nebo organizované skupiny pachatelů, které pak bez většího rizika získají finanční hotovost. Zde opět musí přijít banka s řešením jak uchránit a informovat své klienty. Pro finanční instituce tyto podvody představují další finanční náklady.

Policie k úspěšnému odhalení pachatele potřebuje včasné oznámení a kvalitní informace. To musí zajistit zabezpečovací technika, kamerové systémy a v případě loupežného přepadení na pobočce je nutné svědectví zaměstnanců, kteří jsou pokud možno schopni výpovědi. Pak může Policie včas odhalit pachatele a zabránit mu tak v páchání další trestné činnosti. To je také cílem mé diplomové práce, naučit zaměstnance správnému využívání zabezpečovací techniky, správnému dodržování režimových opatření a uvědomění si jejich nastavení. Dále jsem vypracovala pro zaměstnance postup, který obsahuje postupné kroky

jak se chovat během loupežného přepadení a jak se zachovat těsně po něm. Tyto postupy jsou univerzální a lze je použít na všechny instituce, kde se pracuje s finanční hotovostí.

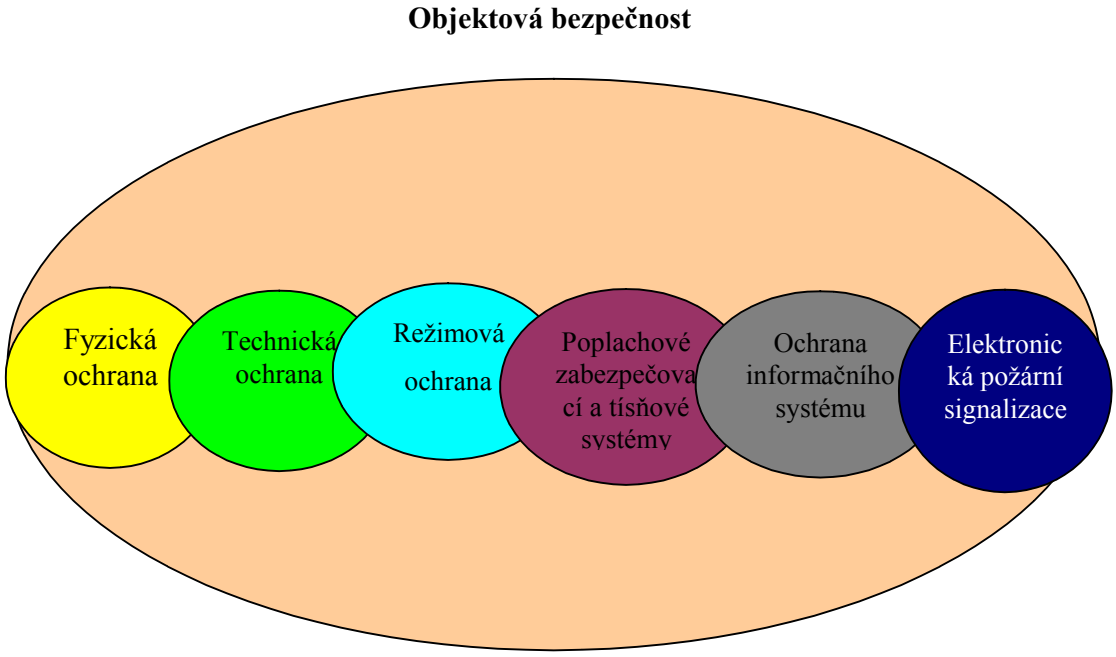
Ve své práci také rozebírám podvody, které se dějí na bankomatech a navrhuji doporučení, jak tyto manipulace a okrádání klientů a bank snížit.

I. TEORETICKÁ ČÁST

1 FORMY SOUČASNÉ OCHRANY OSOB A MAJETKU

1.1 Objektová bezpečnost

Bezpečnost je nevyhnutelnou součástí činnosti každého subjektu. Pod pojmem objektová bezpečnost si můžeme představit nejenom řešení otázek ochrany objektu, ale je zde prioritně zahrnuta ochrana života a zdraví zaměstnanců a osob pohybujících se v objektu, tj návštěvníků, klientů. Musí být zajištěna ochrana informací před nežádoucími osobami a zajištěna ochrana osobních údajů jak zaměstnanců, tak obchodních partnerů. Každá ochrana může být překonána, proto je důležité, aby se systémy ochrany objektů vzájemně doplňovaly. Jedná se zejména o mechanické a stavebně konstrukční zábranné prostředky a poplachový, zabezpečovací a tísňový systém, zajišťující zejména plášťovou, prostorovou a předmětovou ochranu.



Obr. 1. Přehled kombinací ochran a systémů objektové bezpečnosti

1.2 Fyzická ochrana

Fyzickou ostrahu řadíme mezi nejstarší a nejběžnější formu ochrany osob a majetku. Tvoří ji vlastní zaměstnanci nebo zaměstnanci specializovaných bezpečnostních agentur. Fyzická

ostraha patří mezi nejdražší typy ochran. Hlavní úlohu zde hraje lidský faktor, zkušený a profesionálně vycvičený pracovník může včas rozpoznat nebo odhadnout nebezpečí při haváriích, požárech a jiných nenadálých událostech a včasným zásahem odvrátit nebo snížit ztráty. Jejich úkolem je zabránit odcizení a poškození majetku, zabránit neoprávněnému vstupu osob nebo neoprávněnému vjezdu motorových vozidel. [1,3]

Fyzickou ochranu si můžeme rozdělit podle několika hledisek.

1.2.1 Z hlediska časového rozvrhu

- **Nepřetržitá fyzická ochrana** – je vykonávána 24 hodin denně včetně pracovního klidu a svátků
- **Vázaná na pracovní dobu** – ostraha je prováděna jen v pracovní době organizace. Mimo pracovní dobu je objekt střežen pomocí technických prostředků s vyvedeným signálem na pult centralizované ochrany Policie ČR nebo soukromé bezpečnostní služby
- **Nárazová fyzická ochrana** – poskytována mimořádně dle požadavků organizace. U finančních ústavů se tímto období rozumí např. situace po mimořádné události – loupežném přepadení atd.

1.2.2 Podle druhu výkonu

- **Doprovodná** – tato fyzická ochrana se používá u přepravy cenin a větších hotovostí
- **Propustková** – účelem je kontrola vstupu osob do objektu, pracovníci ostrahy vykonávají svou činnost na pevných stanovištích
- **Revírní –** pracovník ostrahy vykonává svou činnost pro více organizací, kde v jednotlivých organizacích se pohybuje v určitých časových úsecích, dle potřeb organizací
- **Aktivní víceúčelová –** jedná se o propojení fyzické ochrany a veškeré dostupné zabezpečovací techniky jako je EZS, EPS, CCTV.
- **Zásahová –** jedná se o výjezdovou skupinu, která provádí kontrolu narušení objektu po aktivaci poplachu.

1.2.3 Podle způsobu zajištění

- **Fyzická ochrana z řad vlastních pracovníků** – nevýhodou je náročnost odborné přípravy zaměstnanců, náklady na výstroj a výzbroj
- **Fyzická ochrana na smluvním základě –** využívá se ke střežení od soukromých bezpečnostních agentur
- **Smíšená fyzická ochrana –** jedná se o kombinaci soukromých bezpečnostních pracovníků, kteří střeží veřejné prostory, např. finančních ústavů, a vlastní zaměstnanci jsou pověřeni hlídáním technologických prostorů.

1.2.4 Podle způsobu výstroje a výzbroje

- **Fyzická ochrana uniformovaná** – pracovní oděv bezpečnostních pracovníků je dám požadavky organizace, kde je prováděno střežení. Organizace mohou mít požadavek na společenský oblek nebo na oděv, který má znaky uniformy.
- **Fyzická ochrana ozbrojená** - v současné době se upouští od nošení zbraní, tento způsob je nebezpečný z hlediska ozbrojené ostrahy, která se první stává terčem útoku útočníka. Zbraň musí být v organizacích, kde se pohybuje veřejnost, nošena skrytě, netýká se příslušníků ozbrojeného sboru, ozbrojené služby nebo ozbrojené složky celní zprávy – zákon o střelných zbraních č. 119/2002 Sb.
- **Fyzická ochrana skrytá (detektivní)** – bezpečnostní pracovník pracuje skrytě, nemá uniformu, jako pracovník fyzické ostrahy. Dění v bance pozoruje skrytě a v případě potřeby zasahuje nebo přivolá pomoc. [8]

1.3 Technická ochrana

Zamezení nebo alespoň znesnadnění přístupu narušiteli do střeženého objektu je úlohou technické ochrany. Využíváme ji i jako bezpečnostní prvek, který nám oznamuje, že došlo k narušení objektu. Střežený objekt si musíme rozdělit do několika úrovní. Důvodem jsou určitá specifika jednotlivých členění střeženého objektu, dle kterých jsou používány mechanické zábranné systémy, dále jen MZS. Mechanické zábranné systémy rozdělíme dle chráněného prostoru do těchto ochranných oblastí:

1.3.1 Obvodová ochrana

Obvodem objektu chápeme vyznačení hranice vlastnického práva k objektu. Ohraničení pozemku může být dáno reliéfem krajiny např. vodním tokem. Dále může být ohraničení provedeno jako nepostradatelná součást zabezpečení nepovoleným vniknutím. Prvky, které nám pomáhají proti neoprávněnému vniknutí, nazýváme mechanickými zábrannými systémy. Patří sem ploty, zdi, ostnaté, žiletkové dráty, brány, branky, podhrabové desky, zastavovací pásy, zpomalovací závory, zpomalovací semafory, turnikety, visací zámky, petlice, atd. Jsou to prostředky, které upozorňují na vstup do vyhrazeného prostoru. [3,8]

1.3.2 Plášťová ochrana

Plášťová ochrana zajišťuje plášť objektu vůči styku s prostorami jiných uživatelů nebo nestřeženými prostorami. Pachatel k neoprávněnému vstupu může použít okna, dveře, mříže, balkónové dveře, sklepní okna, výlohy. Plášťovou ochranu aplikujeme většinou zevnitř objektu. Jedná se obvykle o kombinaci detektorů tříštění skla, magnetických kontaktů detekujících otevření otevíratelných ploch. U velkých prostor je možno využít např. IR závor pro střežení stěn s více vstupy nebo otvory. Můžeme také využít dveřních kukátek, bezpečnostních řetízků. [3,8]

1.3.3 Prostorová ochrana

Má význam pro ochranu důležitých míst ve střeženém objektu. Uvnitř objektu se narušitel již musí pohybovat po hale, chodbách, schodišti. Zabezpečovací systém reaguje na pohyb a na změny v chráněném prostoru. Při výběru zabezpečovací techniky musíme počítat se stářím, s konstrukcí budovy. U starších staveb může docházet k průvanu, otřesům, ke zvukům a vibracím při pohybu vody v potrubích, to vše může vést k falešnému vyvolání poplachu. [3]

1.3.4 Předmětová ochrana

Již názvu je patrné, že předmětová ochrana nám slouží k ochraně a neoprávněné manipulaci s předměty. Zabezpečovací systém spustí poplach po bezprostřední manipulaci s chráněným předmětem. Pro ochranu předmětů, hotovostí můžeme také využít mechanické zábranné prostředky jako jsou trezory, trezorové skříně, příruční pokladny, time-trezory, ohnivzdorné skříně. [3]

1.3.5 Tísňová ochrana

Tísňovou ochranu si rozdělíme na osobní a veřejnou. Osobní nám slouží k vyvolání poplachu u přímého ohrožení při přepadení, ale je také využívána u systému přivolání pomoci u pacientů, při zdravotních problémech. Tlačítka pro spuštění poplachu jsou umísťována na veřejných prostranstvích, obchodních centrech a slouží k vyhlášení poplachu při živelných událostech např. při požáru. [1,3]

1.4 Režimová ochrana

Režimová opatření jsou zpravidla popsána v provozním řádu podniku. Provozní řád může být rozdělena na vnější a vnitřní zásady. Subjekt si může stanovit zásady bezpečnosti objektu a ochrany majetku, bezpečnostní zásady při vstupu a odchodu z objektu, bezpečnostní zásady v pracovní době objektu. Mohou zde být uvedeny režimová opatření vstupu a pohybu osob cizích organizací a dodavatelů, vstupu ozbrojených osob na pracoviště, úklid pracoviště. Velmi důležité je také stanovení klíčového režimu, ve kterém je uvedena správa klíčů a jejich evidence, duplikáty klíčů, postupy při mimořádných událostech atd. [1,3]

1.5 Poplachové zabezpečovací a tísňové systémy

Poplachové zabezpečovací a tísňové systémy jsou řešeny normou ČSN EN 50131, kde jsou definovány jako systémy na detekci vniknutí a indikaci přítomnosti vstupu nebo pokusu „vetřelce“ o vstup do chráněného prostoru. Ve všech stupních zabezpečení termín „vetřelec“ zahrnuje i ostatní typy ohrožení (loupežné přepadení, nebo pohrůžka fyzickým násilím). Poplachový zabezpečovací a tísňový systém by měl být kombinován vhodnými prostředky a postupy fyzické bezpečnosti, aby bylo dosaženo nejvyšší účinnosti. [12]

Norma ČSN EN 50131 nám přesně určuje čtyři stupně zabezpečení

- Stupeň 1: Nízké riziko – předpokládá se, že lupič nebo vetřelec mají malou znalost poplachových zabezpečovacích a tísňových systémů dále jen I&HAS a mají k dispozici omezený sortiment snadno dostupných nástrojů.
- Stupeň 2: Nízké až střední riziko – předpokládá se, že lupič nebo vetřelec mají omezenou znalost I&HAS za použití běžného nářadí a přenosných přístrojů.

- Stupeň 3: Střední až vysoké riziko – předpokládá se, že lupič nebo vetřelec jsou obeznámeni s I&HAS a mají rozsáhlý sortiment nástrojů a přenosových přístrojů.
- Stupeň 4: Vysoké riziko – používá se, má-li zabezpečení prioritu před všemi ostatními hledisky. Předpokládá se, že lupič nebo vetřelec jsou schopni nebo mají možnost zpracovat podrobný plán vniknutí a mají kompletní sortiment zařízení včetně prostředků pro náhradu rozhodujících komponent I&HAS.

Stupeň použitého zařízení a jejich součástí musí odpovídat požadavkům stanoveným při analýze a následném návrhu celého I&HAS.

Využíváme tři typy základních technických prostředků ochrany majetku a osob:

- Elektronické zabezpečovací systémy
- Kamerové systémy
- Systémy kontroly a řízení vstupu

1.5.1 Elektronický zabezpečovací systém

Elektronický zabezpečovací systém dále jen EZS je komplex ústředen, čidel, tísňových hlásičů, prostředků poplachové signalizace, přenosových zařízení, záznamových a ovládacích zařízení.

1.5.1.1 Ústředna

Nejdůležitější součástí celého systému je ústředna, která prostřednictvím detektorů vyhodnocuje a zpracovává informace o pohybu osob nebo jiné informace ze střeženého objektu, při detekci narušení přenáší signál na určené místo.

Ústředna se může nacházet v režimu Vypnuto (DISARMING) - můžeme také říct, že objekt není střežen. Je možný volný pohyb osob po objektu.

V případě, že ústředna je ve stavu Zapnuto (ARMING) – v případě narušení vyhlašuje poplach dle nadefinovaného programu a tento poplach vyvede na pult centrální ochrany. [3]

1.5.1.2 Detektory

Nejčastěji používanými detektory v EZS pro vnitřní použití:

- **Infračervené detektory pohybu (PIR)** – jejich funkcí je detekce infračerveného záření, které vyzařuje narušitel. Při instalaci čidel musíme dbát, aby čidlo nebylo u zdroje sálajícího tepla, na čidlo by také neměly dopadat sluneční paprsky, to vše může způsobovat falešné poplachy.
- **Mikrovlnné detektory pohybu (MW)** – detekuje změny kmitočtu odraženého mikrovlnného signálu od pohybujícího se předmětu, jde o princip Dopplerova jevu, kdy se vyhodnocuje odražená vlna od předmětu. Jde o aktivní detektor, což znamená, že obsahuje vysílač a přijímač mikrovlnného signálu. Mikrovlnné detektory se navzájem ruší, další nevýhodou je pronikání mikrovlnného signálu sklem a tenkými stěnami, jsou náchylné na zářivkové světelné zdroje.
- **Magnetické kontakty** – se skládají z jazýčkového kontaktu a permanentního magnetu. Při otevření oken nebo dveří dojde k přerušení obvodu a tím k vyvolání poplachu.

Obr.2. Magnetický kontakt [14]

- **Detektory rozbití skla** (akustické detektory) – k vyvolání poplachu dojde v okamžiku změny mechanické plochy. Obsahují mikrofon, díky kterému vyhodnocují slyšitelnou část zvuku a tlakovou vlnu, které vznikají tříštěním skla.
- **Otřesové a vibrační detektory** - jsou vybaveny velmi citlivým čidlem, které zachytí i velmi malé otřesy nebo vibrace. Používají se pro střežení zdí, trezorů, kde

může dojít ke vniknutí průrazem stěn a stavebních konstrukci. Detektor zaznamená údery kladivem, sbíječkou, ale zachytí také opakované chvění způsobené řezáním nebo plamenem.

- **Infrazávory** – pracuje na principu vysílací a přijímací strany. Mezi stranami probíhá jeden nebo více infračervených paprsků. V okamžiku, kdy je paprsek přerušen přijímací strana vyhodnotí a vyhlásí poplach.
- **Čidla na ochranu uměleckých předmětů** – mohou to být závěsná čidla, kde předmět je zavěšen na lanku na hák čidla, které vyhodnocuje síly působící na hák. Dále to mohou být polohová čidla, reagují na změnu polohy chráněného předmětu. K chránění nekovových předmětů před přiblížením a dotekem používáme kapacitní čidla. Střežený předmět je v elektrickém poli čidla. Osoba, která je v elektrickém poli mění parametry dielektrika a kmitočet oscilátoru a tím je vyhlášeno narušení.

Obr. 3 Čidlo Michelangelo využití v muzeích [14]

Detektory pro venkovní použití:

- **Infračervené závory a bariéry** – jsou složeny z vysílače a přijímače, mezi kterými prochází jeden nebo více infračervených paprsků. Při přerušení dochází na přijímací straně k vyhodnocení a vyhlášení poplachu.
- **Mikrovlnné bariéry** – tvoří je vysílač a přijímač, mezi kterými se vytváří elektromagnetické pole, které je narušeno, pokud do detekční zóny vstoupí narušitel.

Obr. 4 Mikrovlnná bariéra, ochrana solárních elektráren [14]

- **Štěrbinové kabely** – koaxiální kabel uložený v zemi. Jeden kabel vyzařuje elektromagnetické pole, jehož změny jsou druhým kabelem vyhodnocovány.
- **Mikrofonické kabely –** fungují na principu citlivosti zachvění mikrofonického kabelu. Toto zachvění se přenáší na elektrický signál. Akustický odposlech zjistí charakter narušení a vyhlásí poplach.
- **Zemní tlakové hadice** – základem jsou dvě hadice, které jsou paralelně položené ve vzdálenosti 1 metru od sebe. Hadice jsou napuštěny nemrznoucí kapalinou. Změny jsou vyhodnocování v tlakovém čidle a převáděny na elektrický signál.
- **Perimetrická pasivní infračervená čidla –** jedná se o PIR čidla uzpůsobena pro venkovní prostory. Je zde použita jiná optika, vyhodnocovací zařízení je složitější a je použita klimaticky odolná konstrukce s vytápěným pouzdrem.

1.5.2 Kamerové systémy

Kamerové systémy tvoří nedílnou součást ochrany života, zdraví, majetku a mají také významný preventivní účinek. Tyto systémy se dnes využívají pro monitorování nejrůznějších objektů a pozemků a k následnému uchovávání záznamů na záznamová zařízení.

V současné době můžeme využít dvou typů kamer analogové a IP kamery.

- **Analogové kamery** – v současné době jsou stále velmi rozšířené, i když vyžadují speciální a poměrně drahý převodník obrazu pro připojení k počítači. Signál se v kameře pouze upravuje a poté je kabelem přiváděn v analogovém tvaru na vstup externího převodníku obrazu. V převodníku se signál převádí z analogového tvaru na digitální a poté se po sběrnici PCI přivádí do hlavní paměti PC. Analogový systém využívá koaxiálních kabelů, kdy jeden kabel dokáže přenášet data pouze z jedné kamery. To často vede k rozsáhlým kabelovým vedením.
- **IP kamery** – v IP kamerách se analogový signál získaný ze snímače CCD digitalizuje převodníkem A/D hned v kameře. Kamery zachycují a vysílají živé záběry přímo přes IP síť a umožňuje tak autorizovaným uživatelům lokálně nebo na dálku sledovat, ukládat a spravovat video záběry. Poskytují vyšší komfort užívání i vyšší rozlišení. V IP dokáže jeden síťový kabel přenášet data ze stovek zařízení současně.

Obr. 5 Infračervená válcová kamera IP Bosch [15]

1.5.3 Systémy kontroly a řízení vstupu

V současné době mohou organizace využít plnou integraci systému kontroly a řízení vstupu, který umožňuje mnoho dalších funkcí. Prioritní zůstává regulace přístupu osob nebo vozidel v definovaných prostorových zónách na základě přidělených přístupových práv. Mohou být používány magnetické, čipové, karty, přívěsky - klíčenky, žetony nebo vstupenky, které slouží jako přístupová oprávnění uživateli, kterému bude umožněn vstup nebo vjezd přes elektronické zámky, turnikety, brány, propusti. Systém lze také využít jako

docházkový systém, který slouží k evidenci docházky, sledování pohybu zaměstnanců v průběhu pracovní doby a k přípravě podkladů pro zpracování mzdové agendy.

Také začínají být využívány biometrické informace používané pro identifikaci. Kritéria pro výběr biologické nebo behaviorální vlastnosti člověka určené pro jeho další identifikaci musí splňovat vlastnosti:

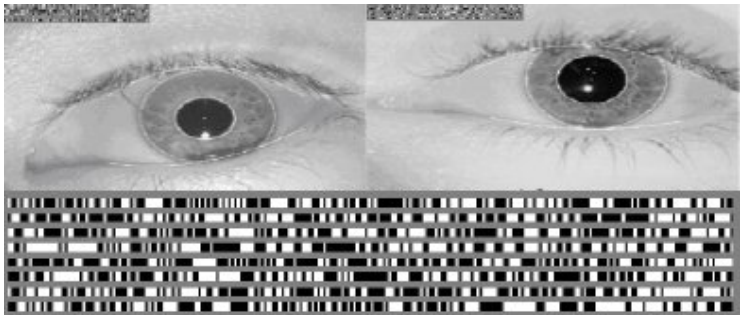
- jedinečnosti, tzn., že se shodná vlastnost nesmí objevit u dvou lidí zároveň,
- univerzálnosti: vlastnost musí být měřitelná u co možná největší skupiny lidí
- trvalosti: vlastnost se nesmí měnit v čase

měřitelnosti: vlastnosti musí být měřitelné shodnými technickými zařízeními

uživatelská přijatelnost: vlastnost musí být snadno a pohodlně měřitelná

Nejlépe prozkoumané a nejvíce rozšířené biometrické vlastnosti používané pro identifikační účely jsou:

- otisk prstu (struktura papilárních linií a jejich detailů)
- dynamika podpisu (rozdíly v tlaku a rychlosti psaní)
- geometrie tváře (vzdálenosti specifických částí – oči, nos, ústa…)
- duhovka oka (obrazový vzorec duhovky)
- sítnice oka (struktura žil na očním pozadí)
- geometrie ruky (rozměry dlaně a prstů)
- struktura žil na zápěstí (struktura žil)
- hlas (tón a zabarvení hlasu)
- DNA, atd.



Obr. 6 Převod obrazu duhovky do el. podoby [13]

1.6 Elektronická požární signalizace

Komplex technických zařízení, které slouží ke včasnému rozpoznání příznaků požáru a vyhlášení požárního poplachu nazýváme Elektronickou požární signalizací dále je EZS. Jedná se o soubor hlásičů požáru, ústředen elektrické požární signalizace a doplňujících zařízení vytvářející systém, kterým se akusticky a opticky signalizuje vzniklé ohnisko požáru a dochází k odeslání hlášení do místa dohledu nad objektem nebo přímo nejbližšímu útvaru Hasičského záchranného sboru. Současně mohou být aktivovány navazující požárně-bezpečnostní zařízení jako jsou únikové východy, odvětrání únikových prostor, požární rozhlas apod. EPS je většinou již integrován do systému EZS. [3]

Ústředna zajišťuje komunikaci s jednotlivými hlásiči požáru a aktivaci výstupních obvodů pro ovládaná koncová zařízení, popřípadě uvádí do činnosti zařízení, která brání rozšíření požáru. Na panelu ústředny nebo na monitoru obsluhy jsou uvedeny informace o celkovém stavu systému o případném požáru v objektu s detailní lokalizací. Na systém EPS je možné navázat systém ozvučení objektu.

- **Opticko-kouřové detektory -** slouží k včasnému odhalení vznikajícího požáru na základě průvodních znaků kouře. U kvalitnějších detektorů je měřicí komora opatřena mřížkou proti nečistotám či létajícímu hmyzu. Částice kouře proniknou do měřicí komory hlásiče, dojde k odrazu vysílaného infračerveného paprsku, takže část záření dopadne na přijímací fotodiodu umístěnou mimo optickou osu vysílací LED. Tato změna je dále zpracována vyhodnocovacími obvody po zakódování je informace o stavu hlásiče - požár, resp. klidový stav - zobrazen LED na hlásiči.
- **Tepelné detektory -** rozpoznají otevřené ohně s kouřem i bez kouře. Detekují okolní teplotu a naměřené hodnoty vyhodnocují podle speciálního algoritmu a

ověřují věrohodnost výsledku testu. Detektor reaguje jak na nárůst teploty, tak i na překročení teplotního maxima. Je možno ho použít i ve zhoršených podmínkách jako je prašnost, kouř nebo pára. LED signalizuje vyhlášení poplachu.

- **Kombinované opticko-kouřové a teplotní hlásiče** - mají stejné parametry jako jednotlivé dílčí detektory a pomocí algoritmu vyhodnocují obě složky požáru - kouř, resp. teplotu. Výhodou tohoto hlásiče je použití dvou hlásičů v jediném provedení.

Obr. 7 Kombinovaný detektor kouře a teplot [14]

- **Ionizační detektory –** jejich funkce spočívá ve vyhodnocení a porovnání dvou komor - referenční, se stopovým obsahem prvku vyzařující záření a měřicí, kam vstupuje kouř. Obě komory jsou porovnávány, pokud dojde k vyrovnání či zvýšení záření obsažené v kouři v měřicí komoře, dojde k vyhlášení poplachu - identifikace pomocí LED. Ionizující záření může být nebezpečné, proto tyto detektory nejsou vhodné do obydlených prostor.
- **Tlakové detektory -** reagují na změnu tlaku v plynu se změnou teploty. Kompresor v pravidelných intervalech vytváří v měřící trubici definovaný přetlak plynu. Řídící logika čidla vyhodnocuje rychlost a směr změny tlaku plynu v detekční trubici. Hlásič je využíván pro těžké průmyslové aplikace v agresivním, popř. výbušném prostředí. Jeho nevýhodou je vysoká pořizovací cena a vysoké provozní náklady.[3]

1.7 Ochrana informačního systému

Informační systém můžeme chápat jako komplex technických prostředků a procesů zabezpečujících sběr, přenos a zpracování dat za účelem vytváření a poskytování informací pro potřeby definovaných uživatelů.

Pro subjekty je velmi důležité chránit své informační systémy a v nich data, která jsou zde uchovávána, zpracovávána a přenášena. To znamená, že musíme chránit informace přenášené mezi počítači, před fyzickými útoky, přírodními katastrofami a vnitřními útoky.

Mezi nejdůležitější prvky softwarového zabezpečení řadíme

- antivirovou ochranu

- ochranu pomocí firewallu

- zálohování dat

- fyzickou ochranu dat [6]

Antivirová ochrana

Škodlivé kódy představují velkou hrozbu pro informační systém, proto je třeba provést opatření proti jejich pronikání do systému, je nutné vytvářet opatření pro řízení přístupů do systému a průběžně informovat uživatele o možných hrozbách. Informací by se měla týkat následující ochranná opatření:

- dodržování softwarových licencí a zákaz používání neautorizovaného softwaru,

- politika ochrany proti hrozbám spojených se získáváním souborů a softwaru přes externí sítě nebo prostřednictvím jiných médií,

- pravidelnou aktualizací a uplatněním detekčních a nápravných softwarů (např. antivirový, antispamový, antispywareový software) na prohlížení počítačů a externích záznamových médií (např. CD, DVD, HDD),

- pravidelné provádění kontrol datového obsahu uloženého v informačním systému,

- plány obnovy činností organizace po napadení škodlivým kódem.

Antivirový program je jeden z nejpoužívanějších ochranných opatření, který se používá proti proniknutí škodlivého kódu. Sleduje vstupně-výstupní místa (elektronickou poštu,

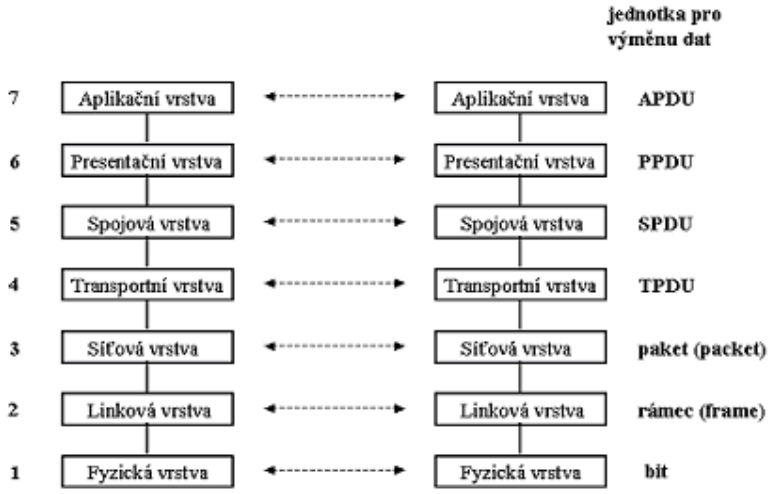
webové stránky nebo přenosná záznamová média), kterými by mohlo dojít k proniknutí do informačního systému. [10]

Firewall

Firewall je zařízení, jehož úkolem je oddělit sítě s různými přístupovými právy a kontrolovat tok dat mezi těmito sítěmi. Kontrola údajů probíhá na základě definování pravidel, které určují podmínky, jaké údaje lze získat z datového toku. Úkolem firewallu je tyto podmínky vyhodnotit a pokud je podmínka splněna provede se akce, která povolí nebo zamítne datový tok.

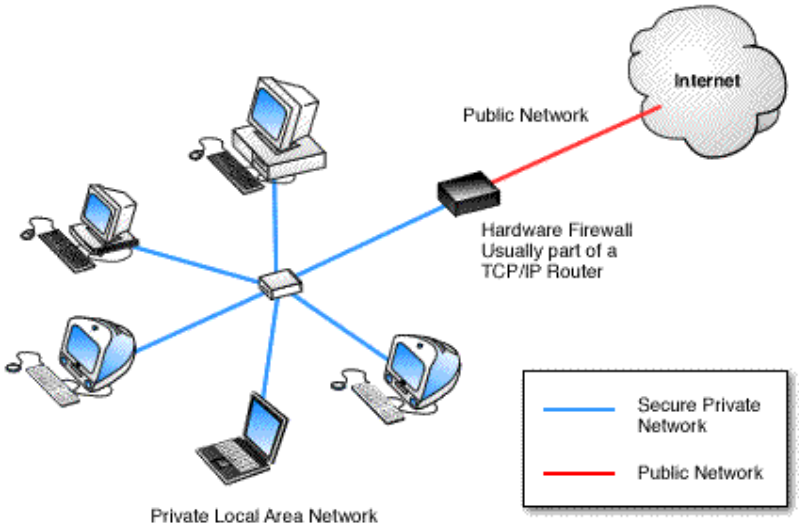
Rozlišujeme firewally Aplikační proxy servery a paketové filtry.

- **Aplikační proxy** server provádí filtrování na aplikační vrstvě referenčního modelu OSI, dokáže přesně analyzovat celý síťový provoz a význam paketů na nejvyšší vrstvě. Nevýhodou je zpomalení síťového provozu.



Obr. 8 Referenční model OSI [9]

- **Paketový filtr** umožňuje sledovat síťový provoz po třetí (čtvrtou) vrstvu modelu OSI (tj. IP adresy a porty). Je sice mnohem rychlejší než proxy, ale jeho správa je komplikovanější a nemá tolik možností. [9]



Obr. 9 Ukázka umístění Firewallu mezi sítěmi [16]

Zálohování dat

Zálohováním ukládáme data z provozních médií na zálohovací média. Podnětem k této činnosti nejčastěji bývá porucha média. Data mohou být také smazána uživatelem, ať již vědomě či nevědomě, ale existuje možnost útoku zvenčí. K takovým patří například neoprávněný přístup či virové napadení. Možností, jak přijít o data, je spousta a poněvadž mohou být některé ztráty nenahraditelné, jeví se zálohování jako optimální řešení.

S ohledem na druh a množství dat určených k zálohování úzce souvisí zálohovací metoda a výběr zálohovacího média, také je nutné vypracovat režim zálohování, to znamená časový plán a pravidelné zálohování. K zálohování souborů, používáme tyto druhy záloh:

- **Normální (úplná) záloha** zkopíruje všechny vybrané soubory na záložní médium a označí je jako zálohované. Toto označení provádí zálohovací program, který všem souborům vynuluje nastavení archivního atributu. Tento druh zálohy je nejjednodušší variantou a také obnova dat je velmi snadná.
- **Přírůstková (inkrementální) metoda**, která dovoluje zálohovat pouze soubory změněné od poslední normální či přírůstkové zálohy. Rovněž ona označuje soubory jako zálohované. Protože se pracuje s menším objemem dat je zálohování rychlejší

Obtížnější je obnova dat, musíme mít k dispozici normální zálohu a pak všechny přírůstkové.

- **Metoda rozdílová (diferenční)** pro obnovu nám postačí pouze normální záloha s poslední diferenční zálohou a soubory se nijak neoznačují.
- **Denní záloha** slouží k zálohování dat vytvořených nebo změněných během dne.

Fyzická ochrana dat

Cílem fyzické ochrany dat je zamezení přístupu neoprávněných osob k jednotlivým komponentům IT systému, jedná se o prostory serveroven a pracovišť správců systémů. Fyzické zabezpečení není pouze zamezení vstupu do místnosti s výpočetní technikou, ale také fyzické zabezpečení HW a SW prvků systému IT.

Je vhodné uložit servery a zálohovací disková pole do uzamykatelných prostorů s omezeným přístupem a navíc je ještě umístit do uzamykatelných racků. Do těchto prostor má pak umožněn přístup pouze přesně stanovený seznam osob s oprávněných ke vstupu, jedná se o:

- serverovny
- datová úložiště
- prostory s klíčovými prvky IT infrastruktury (tj. routery, switche apod.)
- pracoviště správců IT systému

Pokud je vstup možný pouze s odpovědnou osobou, zamezí se vzniku vážných škod při neodborné manipulaci s IT komponenty, IS a zabrání se cílené činnosti s úmyslem poškození systému. [17]

Obr. 10 Rack, nástěnný rozvaděč [18]

2 BEZPEČNOSTNÍ POLITIKA BANKOVNÍHO DOMU

Bezpečnostní politika bankovního domu vychází z bezpečnostní analýzy a obsahuje opatření a metody vybudování komplexního a vyváženého systému ochrany osob, majetku a ochrany bankovního provozu. Představuje návrhy pro vytváření směrnic a postupů při mimořádných událostech. Bezpečnostní politiku můžeme chápat jako soubor řídících, organizačních, technických, personálních a právních instrumentů, které se snaží předcházet, dokumentovat a eliminovat negativní jevy v běžném provozu. Soubor těchto instrumentů má za úkol chránit a bezpečné nakládat s informacemi a s veškerými aktivy, které jsou v bankách ve vlastnictví nebo v jejich péči a to v rámci procesů zabezpečující plynulý chod banky, které musí respektovat vyhlášky České národní banky a zákonné normy České republiky. Pro bankovní domy je udržení určitého bezpečnostního standardu bezesporu právním, podnikatelským a společenským závazkem.

2.1 Operační riziko

Bankovní politikou eliminují finanční ústavy operační rizika. V současné době má operační riziko velký význam, i když existuje již od samého počátku bankovnictví, je to hlavně diky zautomatizovaným bankovním činnostem a rozvoji informačních technologií. Operační riziko v sobě zahrnuje rozsáhlou řadu různých rizik. Česká národní banka označuje operační riziko ve vyhlášce 123/2007 Sb., o pravidlech obezřetného podnikání bank, spořitelních a úvěrových družstev a obchodníků s cennými papíry jako „*riziko ztráty banky vlivem nedostatků či selhání vnitřních procesů, lidského faktoru nebo systémů či riziko ztráty banky vlivem vnějších událostí, včetně rizika ztráty banky v důsledku porušení či nenaplnění právní normy*“. Pokud výše uvedenou definici shrneme, tak se jedná o rizika, která se týkají lidského faktoru, systémů, vnitřních procesů a externích vlivů.

2.2 Cíle bezpečnostní politiky

- Prvořadý cíl Bezpečnost informací – zajištění dostupnosti informací pouze oprávněným osobám, zabezpečení správnosti a kompletnosti informací a metod zpracování. [2]
- Omezit bezpečnostní rizika na přijatelnou úroveň tak, aby se zachovala efektivnost procesů řízení banky.

- Schopnost předcházet a řešit bezpečnostní incidenty je důležitý úkol. K řešení nám vedle metodických postupů pomohou související předpisy a důsledné vyžadovaní zavedených bezpečnostních procedur a procesů v každodenní praxi.
- Vybudování a udržování takového prostředí, které bude odolávat prostředí, ve kterém budou bezpečnostní hrozby rozpoznány a analyzovány dříve než se projeví a způsobí vážné ztráty.

2.3 Vytváření zásad a budování bezpečnostní politiky

Pro vytváření kvalitních zásad bezpečnostní politiky je zajistit trvalou zpětnou vazbu, monitorování a měření rizik, soustavy limitů a omezení. Ve většině bankovních domů tyto úkoly zajišťují příslušné útvary, které zodpovídají za klasifikaci a evidenci aktiv, identifikaci hrozeb, analýzu rizik, implementaci bezpečnostních opatření, které vedou ke snižování rizik a kontrolu. Útvary mají za úkol vytvářet reálné a pružné pravidla, zodpovídají za úplné, jasné a proveditelné definování odpovědnosti, bezpečnostních postupů, které jsou v souladu s právními předpisy. Tyto útvary dle potřeb organizace vytváří výklad bezpečnostních zásad, principů požadavků jako například:

- dodržování legislativních a smluvních požadavků

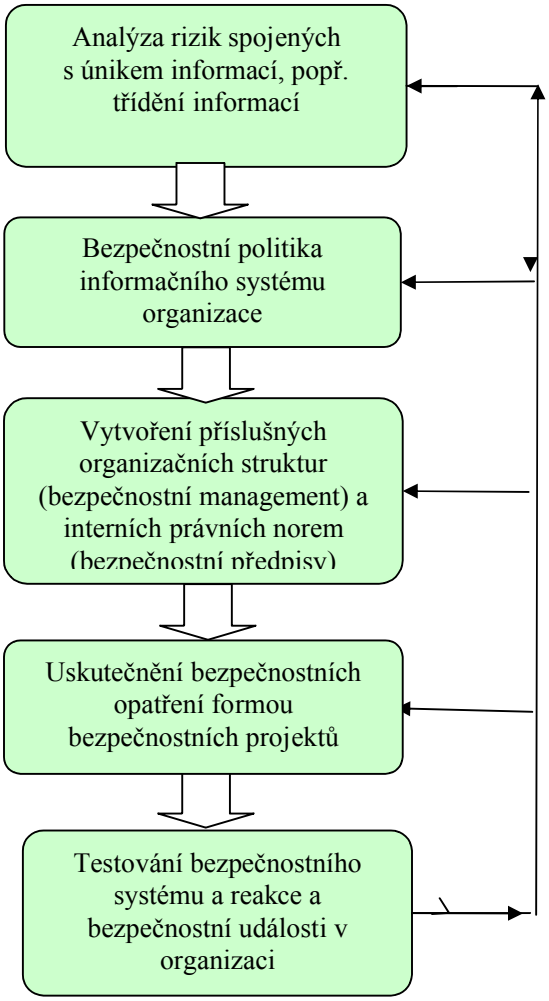
- požadavky na vzdělávání v oblasti bezpečnosti

- principy prevence

- zásady plánování spojitosti informačních činností organizace

- důsledky porušení bezpečnostních zásad.

Dále stanovují obecné i specifické odpovědnosti včetně hlášení bezpečnostních událostí. Vytváří dokumentaci, která přispívá k zajištění bezpečnostní politiky, mohou ze být postupy, které se zaměřují detailněji na specifické informační systémy nebo bezpečnostní pravidla, která musí uživatelé dodržovat.



Obr. 11 Budování informační bezpečnosti [2]

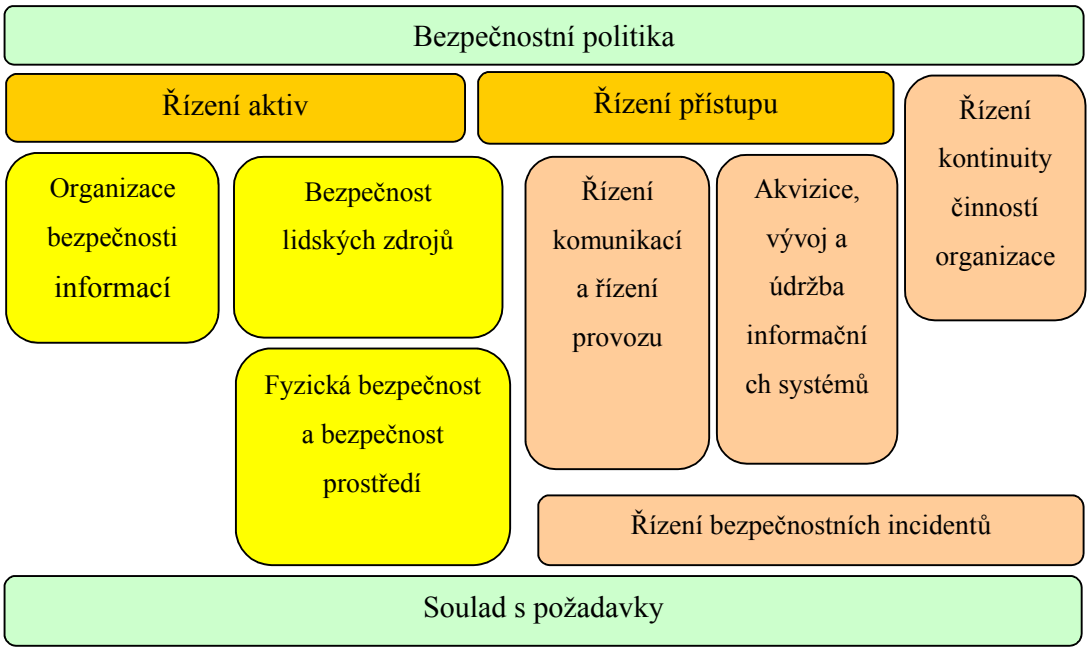
2.4 Základní oblasti bezpečnostní politiky

Bezpečnostní politika vychází z analýzy stavu zajištění bezpečnosti jednotlivých druhů bankovních systémů, produktů a činností. U většiny bankovních domů je ochrana následujících subsystému, které chrání zájmy bank stejná. Jednotlivé oblasti jsou v bankovních domech úzce a vzájemně provázány. Nemohou být použity jeden bez druhého. V rámci eliminace možných bezpečnostních incidentů musí tvořit jeden kompaktní celek.

Jedná se o následující oblasti:

- **Finanční bezpečnost** – opatření k předcházení legalizace výnosů z trestné činnosti a financování terorismu a uplatňování mezinárodních sankcí.
- **Bezpečnost informační technologie** – musí řešit veškerou ochranu informací, jedná se o informace v mluvené i psané formě, nastavení bezpečnostních parametrů a přístupů do systému, ochrana dat, informací v procesu jejich schvalování, testování, celkového zpracování, ukládání a přenosů, zejména při používání telefonů, faxů, počítačových sítí LAN/WAN, internetu [2]
- **Fyzická bezpečnost** – mechanické a technické zabezpečení včetně kamerových systémů, bezpečnost a ochrana zdraví při práci, požární ochrana a ochrana utajovaných skutečností.
- **Bezpečnost v oblasti uložení peněz** - limity pro trezory, pokladny, pravidla pro bezpečné nakládání s hotovostí.
- **Vnitřní bezpečnost –** prevence spočívající ve zdokonalování a správně varování v celé síti bankovního domu, upozorňující na operační rizika a šetření těchto rizik, provádění preventivních kontrol a vyhodnocování operačních rizik.
- **Personální bezpečnost –** dosažení minimalizace příležitostí pro páchání trestné činnosti vlastními zaměstnanci, zajištění předepsaných bezpečnostních školení ve stanoveném rozsahu a stanovených termínech.

Oblasti bezpečnosti informací



Obr. 12 Rozdělení oblastí bezpečnosti informace [2]

Ochrana informací

Ochrana informací je pro bankovní domy zásadní a bankovní domy musí dodržovat zákonná nařízení, kde je uložena povinnost mlčenlivosti, která slouží k ochraně soukromí, jedná se o Zákon č. 101/2000 Sb., o ochraně osobních údajů. V některých případech je vymezen rozsah případů, kdy lze údaje, které jsou chráněny povinností mlčenlivosti sdělit, je zde dokonce uložena povinnost určité skutečnosti oznámit. Dále jsou informace, které nejsou chráněny předpisy, ale jsou pro organizace tak důležité, že se rozhodly tyto informace označit jako důvěrné. Při budování informační bezpečnosti banky je nutné učit důležitost informací a tím i stupeň ochrany. Tyto chráněné informace pak smí používat ty osoby, které je potřebují znát nebo použít ve prospěch organizace, zachování důvěrnosti. Zajistit správnost a kompletnost informací a metod zpracování a dostupnost uživatelům podle jejich potřeby.

Jak zdůrazňuje Smejkal, Rais informace musíme chránit bez ohledu na nosič, na kterém jsou uloženy. Mohou to být audia, videa, fotografie, diskety, pevné disky, paměťová média, paměti počítačů. [2]

2.5 Havarijní plány

Pokud dojde k selhání vnitřních bezpečnostních systémů, musí být připraveny havarijní plány. Jsou to vypracované postupy, které pomáhají snižovat negativní dopady při selhání a minimalizují finanční ztráty. Priorita obnovy systémových zdrojů záleží na obchodní a provozní činnosti společnosti, což určuje prioritu příslušného informačního systému nebo aplikace, která daný systémový zdroj zajišťuje. Tato priorita se stanovuje zejména podle smluvních vztahů, finančních postihů za nedodržení zákonných lhůt, spokojenosti klienta a zachování dobrého jména.

Poněvadž i krátkodobý výpadek může pro společnost znamenat vážné ohrožení, je důležité, aby havarijní plány byly být vypracovány pro všechny provozované činnosti podniku a důkladně informovaly o:

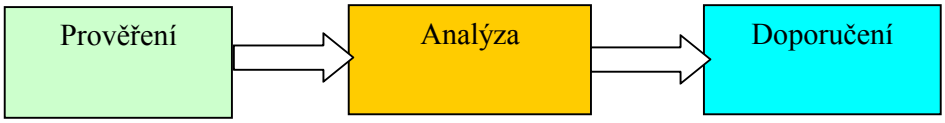
- zvoleném řešení strategie obnovy
- maximální akceptovatelné době výpadku
- seznamu osob řešitelského týmu
- vlastnostech stávajících provozních zařízení
- vlastnostech a umístění náhradních zařízení
- servisních a dodavatelských firmách
- postupech při jednání se státními orgány
- postupech ohledání a zjištění rozsahu škod, pořízení fotodokumentace, případné uzavření obchodního místa

Výsledkem havarijního plánování je vytvoření dokumentu, který obsahuje operační postupy pro zajištění nouzového provozu a dále návrh opatření k obnovení činnosti zasažených systémů a postupy pro přesun pracovních aktivit ze záložních systémů na původní.

2.6 Bezpečnostní audit

Jeden z nejúčinnějších způsobů ověřování bezpečnostního systému je bezpečnostní audit. Zjišťuje správnost nastavení bezpečnostního systému a jejich soulad s obecně závaznými

předpisy. Interní bezpečnostní audit je nástroj vedení organizace a snahou je zvýšit efektivnost a účinnost bezpečnostního systému. Jeho úlohou je předcházet chybám, posléze napravovat chyby, které již nastaly. Zaměřuje se na prevenci systémových nedostatků a na jejich vyhledávání. Provádí se také v případě významných změn v organizaci v případě závažných incidentů (mimořádné události, havárie).



Obr. 13 Průběh bezpečnostního auditu (vlastní obrázek)

- Prověření – shromáždění všech informací pomocí dostupné dokumentace, rozhovorů, samotným pozorováním.
- Analýza – vyhodnocení stavu ze zjištěných skutečností z hlediska rizik, kvalita analýzy určuje platnost závěrů a doporučení.
- Doporučení – návrh nejlepšího opatření k optimalizaci rizik.

3 VNĚJŠÍ BEZPEČNOSTNÍ RIZIKA

Předpokladem úspěšné a efektivní bezpečnostní politiky podniku je schopnost včas a správně vyhodnotit reálné či potenciální bezpečností rizika a hrozby. K tomuto určení nám slouží analýza, která je klíčovým podkladem pro volbu strategií zachování nebo zkvalitnění bezpečnosti ve všech oblastech podniku a je východiskem pro nezaujaté rozhodování a určování priorit v oblasti bezpečnostní politiky. Vzhledem k množství rizik, protože riziko většinou neexistuje samostatně, ale zpravidla se jedná o určité kombinace rizik, je třeba určit prioritu z pohledu dopadu a pravděpodobnosti jejich výskytu a orientovat se na rizikové oblasti. Chceme-li mít rizika pod kontrolou, omezovat je, musíme znát zdroje nebezpečí, charakter a pravděpodobné následky. K tomuto nám slouží analýza rizik. [2]

3.1 Analýza rizik

Analýza rizik zahrnuje identifikaci a posouzení faktorů, které mohou narušit jednotlivé činnosti a cíle organizace. Její podstata spočívá v určení zdrojů rizika, vypracování možných scénářů, určování pravděpodobnosti, následků a vyčíslení finančních nákladů v případě vzniku nežádoucích událostí.

V současné době se již pro analýzu a hodnocení rizik využívá řada metodik a také softwarových nástrojů, které jsou založeny na fyzikálních modelech, na kterých také závisí spolehlivost a správnost výsledků. Uživatel musí nejdříve určit cíle hodnocení rizik a vyhodnotit, zda podklady mají vypovídající hodnotu a lze z nich určit požadovaná rizika. Každá metoda analýzy rizik je pouze pomocný nástroj, to nejdůležitější rozhodnutí závisí na znalostech a zkušenostech člověka.

3.2 Základní pojmy analýzy rizik

- **Aktivum** – jsou to pro podnik všechny hodnoty, které-se mohou působením hrozby snižovat. Předmětem analýzy rizik není aktivum, na které nepůsobí žádná hrozba.
- **Hrozba** – pod hrozbou si můžeme představit přírodní katastrofu, krádež zařízení, neoprávněné získání informací, chybu zaměstnance. Jedná se o události, které mohou způsobit škodu.
- **Zranitelnost** nám vyjadřuje jak citlivé je aktivum na působení dané hrozby. Zranitelnost můžeme také vyjádřit jako slabinu, které může hrozba využít.

- **Protiopatření –** je to návrh s cílem předejít vzniku škody, nebo zmírnit následky vzniklé škody. Výběr protiopatření závisí na pořizovacích nákladech a požadované efektivitě.
- **Riziko –** nám vyjadřuje míru ohrožení aktiva, nebezpečí vzniku škody, poškození, ztráty nebo zničení, popřípadě nezdaru při podnikání. [2]

3.3 Obecný postup analýzy rizik

- **Stanovení hranice analýzy rizik –** zde se musí rozdělit aktiva, která je nutné analyzovat a aktiva, na která nepůsobí žádná hrozba, popřípadě vzhledem k hodnotě aktiva není nutné aktivum zahrnovat do analýzy.
- **Stanovení hodnoty a seskupování aktiv –** hodnota aktiva závisí na velikosti škody způsobené zničením nebo ztrátou tohoto aktiva. Pokud je aktiv velké množství, seskupují se aktiva dle podobných vlastností a tím se sníží jejich počet. Seskupují se aktiva obdobné kvality, hodnoty, účelu, užívání.
- **Identifikace hrozeb –** jsou vybrány takové hrozby, které by mohly způsobit škodu alespoň jednomu z aktiv subjektu. Výběr hrozeb záleží na subjektu, na jeho poloze (periferie města, střed města, kriminalita v místě sídla subjektu). Ohrožení přírodními hrozbami (záplavy, požáry, tornáda), o jaký podnikatelský subjekt se jedná, jeho konkurence a postavení na trhu, hospodářské výsledky, další podnikatelské záměry.
- **Analýza hrozeb a zranitelností** – principem je hodnocení jednotlivých hrozeb proti jednotlivým aktivům. Určí se zranitelnost aktiva k určité hrozbě a naopak a jsou zde brána v úvahu realizovaná protiopatření.
- **Pravděpodobnost jevu –** při neurčitosti, zda zkoumaný jev nastane musíme doplnit údaj s odhadem s jakou pravděpodobností může jev nastat.
- **Měření rizika –** riziko je v určitých situacích větší, což vyplývá z ceny aktiva, zranitelnosti tohoto aktiva a úrovně hrozby. Mnohdy pracujeme s veličinami, které nelze přesně měřit, zde se musíme spolehnout na kvalifikovaný odhad a na zkušenosti odborníka. [2]

3.4 Základní metody pro stanovení analýzy rizik

Jedním ze základních kritérií volby nevhodnější metody analýzy rizik je dostupnost dat, které umí metoda zpracovat. Každá z existujících metod pro stanovení rizik byla vytvořena pro určitý specifický úkol.

Mezi základní metody řadíme kvantitativní a kvalitativní analýzu.

3.4.1 Kvantitativní analýza rizik

Uplatňuje hlavně v oblasti bezpečnosti organizací a jejich informačních systémů, jsou založeny na pravděpodobnosti výskytu jevu a pravděpodobnosti ztráty hodnoty.

Smejkal a Rais popisují nejznámější metody kvantitativní analýzy, mezi které patří:

- **Metoda CRAMM** (*CCTA Risk Analysis and Management Methodology*) – jedná se pravděpodobně o nejznámější metodu, u které se provádí ohodnocení systémových aktiv, seskupení aktiv do logických skupin a stanový se hrozby, které působí na tyto skupiny. Provede se prozkoumání zranitelnosti systému a stanový se požadavky na bezpečnost pro jednotlivé skupiny. To je základem pro navržení bezpečnostních opatření.
- **Metodika @RISK** využívá k analýze rizik simulačních metod Monte Carlo. Jedná se o zpracování ve formě tabulek. V této metodě se pak nejisté hodnoty zaměňují funkcemi, které určují rozsah možných hodnot. Vybrané souhrnné hodnoty pak představují nástroj pro další rozhodování.
- **Metodika RiskPAC** slouží k automatizaci dotazníkových přístupů. Tato analýza zahrnuje techniky, které zpracovávají odpovědi na základě dotazníků a poskytují podklady pro vytvoření závěrů.
- **RiskWatch** metoda, která poskytuje metodický soubor pro zjištění, simulaci a následnou změnu parametrů jednotlivých rizik systému. Využívá se vytvoření modelu ze získaných dat nebo simulační metody Monte Carlo. Oba přístupy lze různě spojovat a doplňovat. Výsledky jsou získány na základě souborů otázek, seřazených podle určených bezpečnostních oblastí. [2]

3.4.2 Kvalitativní analýza rizik

Je založena na přesném matematickém výpočtu rizik z četnosti výskytu incidentů a jejich dopadů. Tato metoda poskytuje přesnější výsledky, jsou však časově a finančně náročné. Výsledkem je souhrn opatření, jejich cena a čas potřebný k realizaci. Podle Smejkala a Raise je nejběžnější Metoda účelových interview (Metoda Delphi).

- **Metoda účelových interview (metoda Delphi)** – využívá se zde soubor otázek, které jsou rozeslány mezi odborníky, kteří řeší daný problém. Při řešení otázek nedochází k vzájemnému ovlivňování, protože odpovídající při zpracování otázek nepřichází do styku. Při rozdílných odpovědích jsou vypracovány další otázky, ale jenom ke sporným otázkám. Odpovědi jsou pak dále znovu posuzovány. V rámci metody Delphi se používají i jiný obměněné varianty, například metoda anketní analýzy, metoda scénářů. [2]

Naopak Tichý preferuje v mnoha fázích analýzy rizik stromové diagramy. Konstatuje, že je lze využít k odhadu pravděpodobnosti výskytu sledovaného jevu. Diagram rozhodovateli usnadňuje přehled v pravděpodobnostech vzniku jednotlivých událostí, příčin a následků. Stromové diagramy uvádí v těchto formách:

- **Stromy událostí** – analýzou se sleduje zjištění vývoje procesu výrobního, politického, rozhodovacího. Přitom události mohou, ale také nemusí být poruchami.
- **Stromy poruch** – uplatňují se tam, kdy se při skutečné poruše hledají její příčiny a vyvozují závěry pro prevenci rizik nebo pro jiná rozhodnutí.
- **Stromy příčin** – hledají se příčiny událostí, které, které již vznikly nebo teprve mohou nastat.
- **Diagramy následků** – hledají se následky jedné nebo několika událostí, které již nastaly nebo mohou nastat.

Musím souhlasit s Tichým, když konstatuje, že existence rizika může být pro subjekt hrozbou, ale také příležitostí. Je jedním z autorů, kteří mezi analýzy zahrnuje i analýzu SWOT.

- **Analýza SWOT –** je založena na identifikaci základních faktorů, kterými jsou:

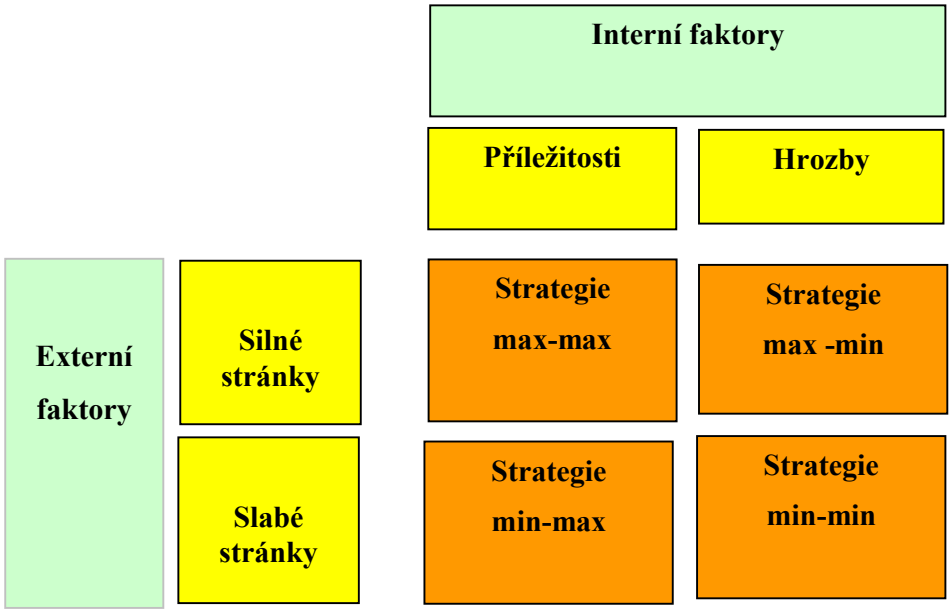
- silné stránky (Strengths)

- slabé stránky (Weaknesses)

- příležitosti (Opportunities)

- hrozby (Threats)

Cílem analýzy je získat přehled o možnostech snížení pravděpodobnosti hrozby a zvýšení pravděpodobnosti příležitosti pro subjekty. Tým je sestaven zpravidla z řad pracovníků organizace, poněvadž jsou obeznámeni se stavem organizace a prostředím. Na obrázku 4 je znázorněna možná struktura analýzy SWOT.



Obr. 14 Struktura analýzy SWOT [2]

V technické praxi existuje celá řada metod pro analýzy rizik. Autoři ve svých publikacích mají vypracovány metodiky, o kterých si myslí, že jsou nejpoužívanější. Ucelený přehled metodik zpracovalo MV ČR Generální ředitelství HZS ČR. Charakteristika obvykle používaných postupů je následující:

- **Check List (kontrolní seznam)** - je postup založený na systematické kontrole plnění předem stanovených podmínek a opatření. Seznamy kontrolních otázek jsou zpravidla generovány na základě seznamu charakteristik sledovaného systému nebo

činností, které souvisejí se systémem a možnými dopady, selháním jednotlivých součástí systému a vznikem škod. Struktura seznamu je flexibilní, lze ji měnit od jednoduchého seznamu až po složitý formulář, který umožňuje zahrnout různou důležitost, váhu parametru v rámci daného souboru.

- **Safety Audit (bezpečnostní kontrola)** – tímto postupem se hledající rizikové situace a navrhují se opatření na zvýšení bezpečnosti. Metoda představuje postup hledání možné nehody nebo provozního problému, který může nastat v posuzovaném systému. Formálně je používán připravený seznam otázek a matice pro skórování rizik.
- **What – If Analysis (analýza toho, co se stane když)** - je postup na hledání možných dopadů vybraných provozních situací. V podstatě je to spontánní diskuse a hledání nápadů, ve které skupina zkušených lidí dobře obeznámených s procesem klade otázky nebo vyslovuje úvahy o možných nehodách. Není to vnitřně strukturovaná technika jako některé jiné (např. HAZOP a FMEA). Namísto toho po analytikovi požaduje, aby přizpůsobil základní koncept šetření určitému účelu.
- . **Preliminary Hazard Analysis – PHA (předběžná analýza ohrožení)** – také kvantifikace zdrojů rizik je postup na vyhledávání nebezpečných stavů nebo nouzových situací, jejich příčin a dopadů a na jejich zařazení do kategorií dle předem stanovených kritérií. Koncept PHA ve své podstatě představuje soubor různých technik, vhodných pro posouzení rizika.
- . **Process Quantitative Risk Analysis – QRA (analýza kvantitativních rizik procesu)** - je systematický a komplexní přístup pro predikci odhadu četnosti a dopadů nehod pro zařízení nebo provoz systému. Analýza kvantitativních rizik procesu je koncept, který rozšiřuje kvalitativní (zpravidla verbální) metody hodnocení rizik o číselné hodnoty. Algoritmus využívá kombinaci (propojení) s jinými známými koncepty a směřuje k zavedení kritérií pro rozhodovací proces, potřebnou strategii a programy k efektivnímu zvládání (řízení) rizika. Vyžaduje náročnou databázi a počítačovou podporu.
- **Hazard Operation Process – HAZOP (analýza ohrožení a provozuschopnosti)** – je postup založený na pravděpodobnostním hodnocení ohrožení a z nich plynoucích rizik. Jde o týmovou více oborovou metodu. Hlavním cílem analýzy je

identifikace scénářů potenciálního rizika. Odborníci se pomocí brainstormingu. soustřeďují na posouzení rizika a provozní schopnosti systém

- **Event Tree Analysis – ETA (analýza stromu událostí) –** jedná se o grafícko-statistická metodu. Názorné zobrazení systémového stromu událostí představuje rozvětvený graf s dohodnutou symbolikou a popisem. Znázorňuje všechny události, které se v posuzovaném systému mohou vyskytnout. Podle toho jak počet událostí narůstá, výsledný graf se postupně rozvětvuje jako větve stromu.
- **Failure Mode and Effect Analysis – FMEA (analýza selhání a jejich dopadů) – v**využívá se především pro vážná rizika a zdůvodněné případy. Vyžaduje aplikaci počítačové techniky, speciální výpočetní program, náročnou a cíleně zaměřenou databázi.
- **Fault Tree Analysis – FTA (analýza stromu poruch) –** analýza využívá zpětného rozboru událostí za využití řetězce příčin, které mohou vést k vybrané cílové události. Metoda FTA je graficko analytická popř. graficko statistická metoda. Proces dedukce určuje různé kombinace hardwarových a softwarových poruch a lidských chyb, které mohou způsobit výskyt specifikované nežádoucí události na vrcholu.
- **Human Reliability Analysis – HRA (analýza lidské spolehlivosti)** - je postup na posouzení vlivu lidského faktoru na výskyt pohrom, nehod, havárií, útoků nebo následky některých jejich dopadů. Analýza HRA má těsnou vazbu na aktuálně platné pracovní předpisy především z hlediska bezpečnosti práce.
- **Fuzzy Set and Verbal Verdict Method – FL-VV (metoda mlhavé logiky verbálních výroků) -** je metoda založená na jazykové proměnné. Jde o vícehlediskovou metodu rozhodovací analýzy z kategorie měkkého, mlhavého typu. Opírá se o teorii mlhavých množin a může být aplikována v různých obměnách, jednak samostatně s přímým výstupem priorit, anebo jako stupnice v pomocných bodech [PB], namísto standardní verbálně-numerické stupnice v relativních jednotkách [RJ], tj. ve spojení s metodou TUKP – Totálního ukazatele kvality prostředí (možnost uplatnění axiomatické teorie kardinálního užitku). Umožňuje aplikaci jednotlivcem i v kolektivu.

- **Relative Ranking – RR (relativní klasifikace)-**jedná se spíše o analytickou strategii než o jednoduchou dobře definovanou analytickou metodu. Tato strategie umožňuje analytikům porovnat vlastnosti několika procesů nebo činností a určit tak, zda tyto procesy nebo činnosti jsou natolik nebezpečné, že to analytiky opravňuje k další podrobnějšímu zkoumání. Relativní klasifikace může být použita rovněž pro srovnání několika návrhů umístění procesu nebo zařízení a zajistit tak informace o tom, která z alternativ je nejlepší nebo méně nebezpečná. Tato porovnání jsou založena na číselných srovnáních, která reprezentují relativní úroveň významnosti každého zdroje rizika.
- **Causes and Consequences Analysis - CCA (analýza příčin a dopadů) -**je směs analýzy stromu poruch a analýzy stromu událostí. Největší předností CCA je její použití jako komunikačního prostředku:diagram příčin a dopadů zobrazuje vztahy mezi koncovými stavy nehody (nepřijatelnými dopady) a jejich základními příčinami. Protože grafická forma, jež kombinuje jak strom poruch, tak strom událostí do stejného diagramu, může být hodně detailní, užívá se tato technika obvykle nejvíce v případech, kdy logika poruch analyzovaných nehod je poměrně jednoduchá. Jak už napovídá název, účelem analýzy příčin a dopadů je odhalit základní příčiny a dopady možných nehod. Analýza příčin a dopadů vytváří diagramy s nehodovými sekvencemi a kvalitativními popisy možných koncových stavů nehod.
- **Probabilistic Safety Assessment – PSA (metoda pravděpodobnostního hodnocení)** – je to metoda, která určuje slabá místa částí systému k celkové zranitelnosti celého systému. Tato technologie se používá např. k modelování scénářů předpokládaných jaderných havárií. Metodika PSA se skládá z: pochopení systému jaderného zařízení a ze shromáždění důležitých dat o jeho chování při provozu; identifikace iniciačních událostí a stavů poškození jaderného zařízení; modelování systémů a řetězců událostí pomocí metodiky založené na logickém stromu; hodnocení vztahů mezi událostmi a lidskými činnostmi; vytvoření databáze dokumentující spolehlivost systémů a komponent. [19]

Pokud zadáme přesné požadavky na bezpečnostní posouzení vnější bezpečnostních rizik můžeme díky metodám analýzy rizik získat detailní analýzu ukazatelů, které potřebujeme řešit. Která z vypsaných metod je vhodná pro posouzení vnějších bezpečnostních rizik?

Toto posouzení jsem nechala na samotný závěr kapitoly a výsledek je zpracován v tabulce č.1. Podotýkám, že vybrané analytické metody jsou dle mého názoru a postavené na teoretickém základu, dle dostupné literatury.

Tab. 1. Využití metod analýzy rizik

Otázky k řešení	**Metody analýzy rizik**	**Check List**	**Safety Audit**	**What – If Analysis**	**Preliminary Hazard Analysis – PHA**	**. Process Quantitative Risk Analysis – QRA**	**Hazard Operation Process – HAZOP**	**Event Tree Analysis – ETA**	**Fault Tree Analysis – FTA**	**Human Reliability Analysis – HRA**
Analýza vnějších vlivů		x	x	x	x	x	x	x	x	
Audit současných bezpečnostních systémů		x	x	x	x	x	x	x	x	_
Analýza rizik		x	x	x	x	x	x	x	x	_
Režimová opatření		_	_	_	_	_	_	x	x	x
Kriminalita v dané oblasti		_	_	_	_	x	_	_	_	_
Profil pachatele		_	_	_	_	_	x	x	_	x

II. PRAKTICKÁ ČÁST

4 OCHRANA PŘEPÁŽKOVÝCH PRACOVIŠŤ

Ochrana hodnot a zájmů jsou ohrožovány incidenty, které mají nežádoucí vliv na požadovaný stav a plynulý proces v bankovních domech. Tyto incidenty, které můžeme také nazvat hrozbami, musíme považovat za trvalá rizika, která nelze odstranit, ale musíme se pokusit je co možná nejvíce snížit. Převládající charakter zmíněných rizik je dán povahou činností nabízených služeb, které se na konkrétním přepážkovém pracovišti poskytují. Při posuzování nebezpečnosti jednotlivých druhů rizik musíme vycházet z následků jednotlivých mimořádných událostí. Výsledkem je vytvoření bezpečnostního systému, kde prioritou je ochrana života a zdraví osob před jinými hodnotami. Mezi rizika, která nejvíce ohrožují životy a zdraví zaměstnanců a klientů bank patří loupežná přepadení, která můžeme předvídat v místech, kde je běžná manipulace s hotovými penězi. Vzhledem k závažnosti následků nelze tento druh ohrožení srovnat s jinými majetkovými riziky, poněvadž zahrnuje prvky násilí vůči zaměstnancům i dalším osobám. Tyto události zvyšují společenskou nebezpečnost této trestné činnosti, a proto se banky snaží uplatňovat a zdokonalovat systém schopný zajistit ochranu před tímto rizikem.

Mimořádná událost se svou povahou, průběhem a dopadem vymyká z běžné pracovní činnosti a má dopad na životy či zdraví zaměstnanců a klientů. Jedná se již o výše uvedená loupežná přepadení, ale také vloupání nebo technickou poruchu narušující plynulý provoz, dále sem patří živelné pohromy, požár apod.

Tab. 2 Loupeže na finančních institucích v roce 2009 - 2011

Rok	Počet loupeží	Objasněno	Neobjasněno	Objasněno v %
2009	172	76	96	44,18
2010	145	66	79	45,51
2011	120	68	52	56,66

4.1 Nejčastější způsoby provedení loupeží

Vybavení a postupy pachatelů zpravidla odpovídají určitým podmínkám vybraného místa přepadení. Na způsobu provedení loupeže závisí stavební dispozice, členění vnitřních prostor, jejich zabezpečení viditelnými prvky, provedení interiéru a provozní režim banky. Zvolený postup loupeže se pak snaží překonat nebo obejít zjevné překážky a systém

bezpečnostních opatření jak technického tak organizačního charakteru. U každé provedené loupeže musí proběhnout:

- začátek loupežného přepadení
- způsob získání hotovosti
- postup opatření před útěkem
- pro útočníka je velmi důležitá co nejkratší doba provedení

Zahájení loupežného přepadení může probíhat přímo v otevírací době pobočky banky, kdy jsou zaměstnanci banky ohrožováni na svých pokladních místech přes přepážku nebo pachatelé využijí situace, kdy zaměstnanec musí opustit chráněný prostor přepážky. Jde především o situace při příchodu a odchodu zaměstnanců, tedy při odemykání a zamykání prostor pobočky před začátkem a koncem provozní doby, nebo v době polední pauzy.

Útočník se sám snaží si vytvořit nejlepší podmínky pro zahájení útoku. Až do okamžiku přepadení se pokouší krýt svůj záměr vystupováním pod předem připravenou historkou, kterou chce vylákat zaměstnance mimo chráněný prostor, nebo naopak do těchto prostor proniknout sám. Většinou se vydávají za zaměstnance servisních a různých dodavatelských firem, ale mohou se také vydávat za policisty, státní dozory apod. Důležitá je věrohodnost hrané situace, aby způsobila ochotné a vstřícné jednání zaměstnanců banky.

Další variantou přepadení může být nátlak k vydání hotovosti ohrožováním třetí osoby, obvykle klienta, který se nachází v prostoru pobočky. Může se jednat o naplánovanou taktiku, nebo zkratové jednání pachatele. Jedná se většinou o útoky se zbraní.

Ve většině případů loupeže se pachatel snaží o získání hotovosti, aniž by jednání bylo zpozorováno ostatními zaměstnanci nebo klienty. Toto přepadení probíhá bez vnějších příznaků přepadení. Pachatel není maskován nebo jen částečně (sluneční brýle, čepice s kšiltem, paruka), místo slovního projevu používá výhružku v podobě papírku s napsaným požadavkem. Držení zbraně naznačuje rukou skrytou v oděvu nebo zbraň na krátkou chvíli ukáže, popřípadě položí na přepážku krabičku, pod pohrůžkou nástražného výbušného systému.

Dále mohou pachatelé využít moment překvapení. Útok může být proveden i bez přímého ohrožování zaměstnanců nebo klientů. Útočník nemusí být ozbrojen, vnikne do zázemí přeskočením přepážky, překonáním nástavby a hotovost si z pokladny vezme sám.

Zaměstnanci většinou v úleku odstoupí od svých pracovišť, takže nedochází k fyzickému ani slovnímu kontaktu s pachateli.

Dalším způsobem provedení loupežného přepadení je ozbrojený útok na přepravu hotovostí, pokud je tato přeprava prováděna vlastními zaměstnanci. V případě bank mohou být součástí přepravy i dotace bankomatů umístěných mimo vlastní objekty banky. Bankomaty můžeme považovat za pokladní místa, u kterých je zajištění ochrany při jejich plnění hotovostí značně ztížené. Proto jsou operace spojené s obsluhou bankomatů jednou z nejvíce ohrožených činností dotujících zaměstnanců.

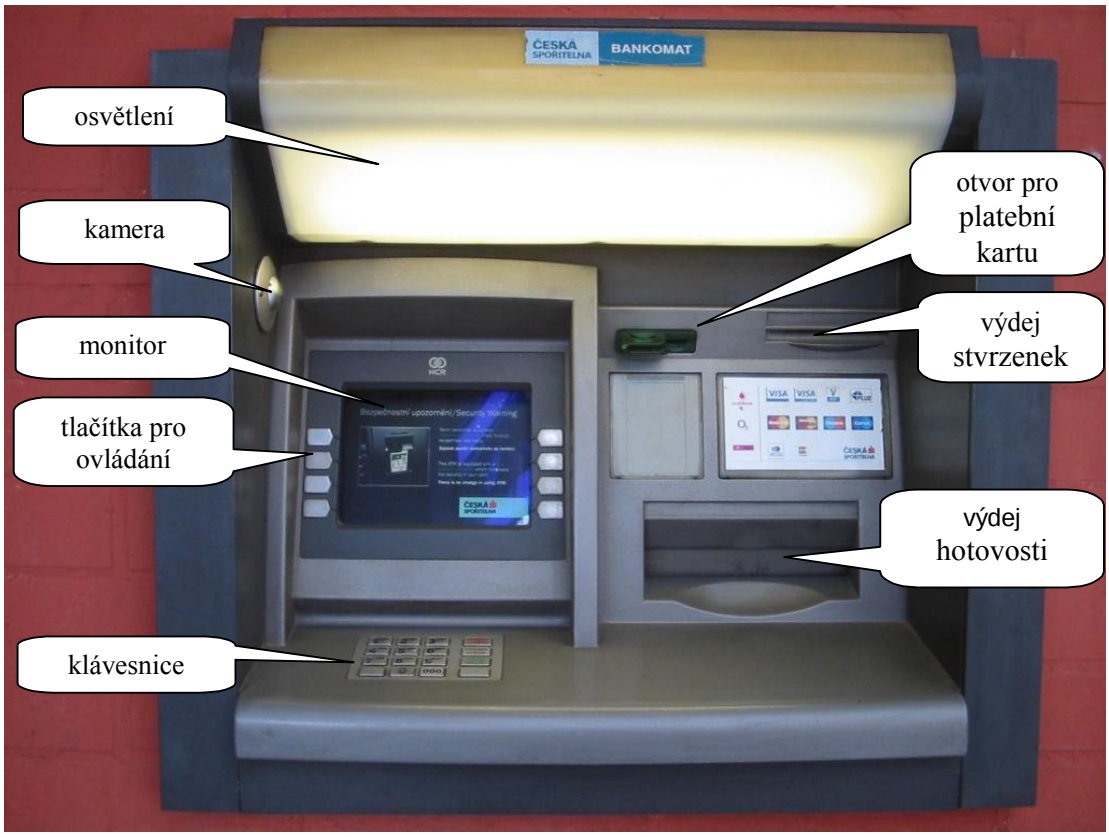
Pachatelé odcizí peněžní hotovost klientům odcházející s vybraným peněžním obnosem z pokladního místa. K odcizení může dojít loupežným přepadením nebo krádeží. V obou případech je nutné vytipování, které může probíhat ve vnitřních, veřejně přístupných prostorách banky, nebo z vnějšího prostředí, jehož dispozice dovoluje vizuální přehled o klientech provádějících výběr. K této trestné činnosti může docházet pouze u některých pracovišť, jejichž vnitřní nebo vnější prostory jsou členěny způsobem umožňujícím provádět tuto činnost nepozorovaně.

Obr. 15 Přepážkové pracoviště banky (vlastní snímek)

4.2 Bankomaty

Další možností jak získat hotovost je výběr peněz přes bankomaty. Zde musí mít pachatelé technické znalosti. Nejedná se většinou o práci jednotlivce, ale o organizované skupiny lidí. Ti tuto aktivitu vyvíjejí bez vědomí klientů a banky. Klient si většinou všimne neoprávněné transakce na výpisu až o několik dní později, nebo je okraden v době, kdy jde reklamovat nevydání hotovosti nebo platební karty do banky.

Bankomaty jsou vybaveny autorizačním systémem, který ověřuji správnost PINu a pravost informací na platební kartě. V současné době je většina platebních karet, které jsou u nás klientům vydávány, magnetická tj. údaje jsou uloženy v magnetickém proužku. Začínají se také objevovat hybridní platební karty, kdy tyto karty jsou opatřeny čipem. Důvodem tohoto kroku banku je znesnadnění kopírování platebních karet, protože v současné době dochází k nárůstu výskytu kopírovacích zařízení.



Obr. 16 Popis čelního panelu bankomatu (vlastní snímek)

Možnosti zneužití, které vedou k zneužití platební karty klienta jsou následující:

4.2.1 Dočasné znepřístupnění výdeje bankovek

Tento poměrně jednoduchý způsob okradení klientů je založen na zaslepení otvoru pro vydání hotovosti oboustrannou fólií, na které může být nalepena lišta vypadající jako falešná dvířka. Bankomat vyzve k odběru peněz, ale ty zůstanou nalepeny na spodní straně lišty. Klienta nenapadne, že se mohl stát obětí podvodu a vydá se do své banky reklamovat nevydání hotovosti. V těsné blízkosti již čeká pachatel, který lištu odstraní a odcizí přilepené bankovky.

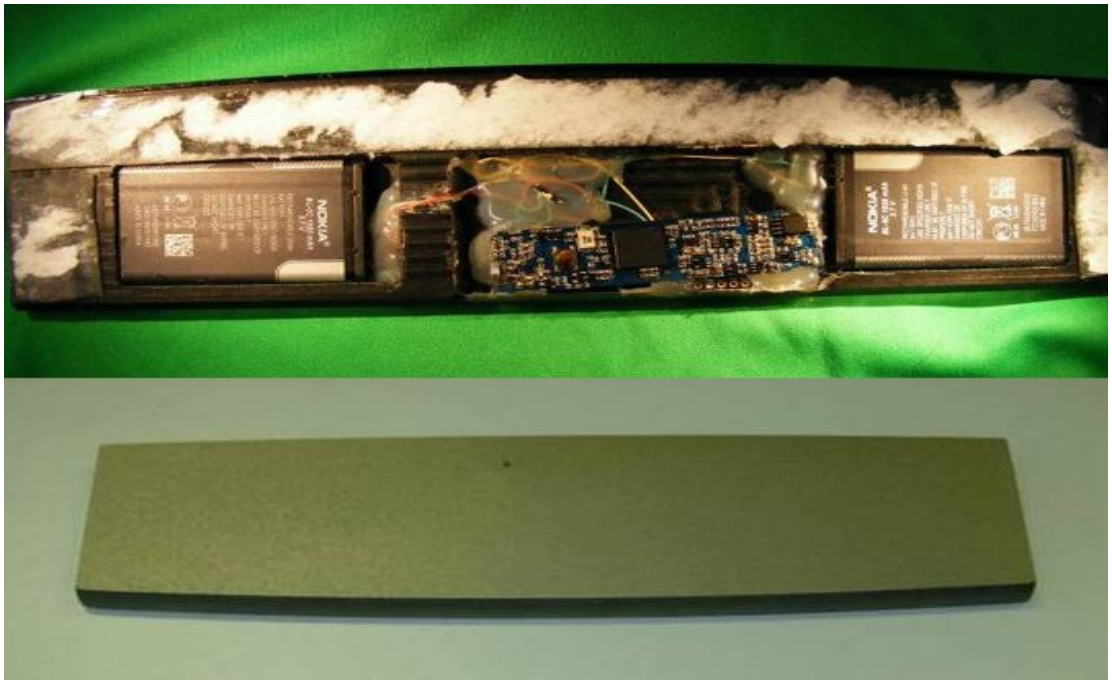
4.2.2 Tepelná fólie

Tato fólie slouží k zaznamenání stisknutých kláves na bankomatu. Klávesnice bankomatu je překryta tenkou průhlednou fólií, která je schopná na základě tepla vydávaného lidským prstem zaznamenat klávesy, které byly použity při zdávání PINu. Po jeho získání pachatelé později platební kartu klientovi odcizí. Tato metoda se používá společně s libanonskou smyčkou nebo skimmingem.

4.2.3 Vestavěná čtečka karet – skimming

Skimmovací zařízení je technické zařízení umožňující zkopírování elektronických údajů z magnetických platebních karet. Taková zařízení bývají nejčastěji nainstalována pachateli na bankomaty v místech pro vkládání karty a to formou různých nástavců napodobující originál nebo formou panelu, který bývá montován na originální součást bankomatu. Skládají se z části, která načítá data z platební karty vložené do bankomatu a části, která umožňuje získat číselný PIN kód, tomu využívají horní panel bankomatu pro umístění minikamery o velikosti řádově v mm, která snímá PIN nebo může být použita falešná klávesnice, která je samostatně, ale i formou celého panelu montována na originální klávesnici či panel bankomatu. Pouze získání obou těchto údajů umožní osobám, které nelegálně kopírují údaje z platební karty, následnou výrobu padělků karet a nelegální výběry z finančních účtů v ČR i v zahraničí.

Kopírovací zařízení a krycí lišty kopírovacích prostředků na bankomatech jsou většinou provedeny v barvě a kovu velmi podobných materiálů, ze kterých je bankomat vyroben.



Obr. 17 Falešný panel bankomatu s kamerou pro snímání PIN kódu [20]

Obr. 18 Nástavec sloužící ke skenování karet [21]

4.2.4 Zabavení karty bankomatem – libanonská smyčka

Pachatelé vloží do otvoru na vkládání platebních karet kousek přeloženého pásku, který přilepí k okrajům otvoru nebo falešnému rámečku. Jakmile se bankomat bude snažit vysunout kartu zpět, karta uvízne ve vložené smyčce. Většina klientů odchází reklamovat zadrženou kartu v bankomatu. V blízkosti již čeká podvodník, který za pomocí pásku

vytáhne ukradenou kartu. PIN získá pomocí falešné klávesnice, minikamery, tepelné fólie atd.

4.3 Technické požadavky na návrh poplachového systému pro detekci vniknutí a přepadení

Při návrhu poplachového systému musíme vycházet z ČSN EN 50131-1 a předpisů pojišťoven, kde výsledkem je zařazení objektu do kategorie stupně zabezpečení a z toho nám vyplyne optimální doporučená ochrana objektu. Pro přehlednost uvádím dvě tabulky. Tabulka č. 3 nám zobrazuje stupně zabezpečení a objekty, kterých se tento stupeň týká. V tabulce č. 4 je uvedena doporučená ochrana s ohledem na již uvedené stupně zabezpečení. Na bankovní domy se vztahuje stupeň zabezpečení 3.

Tab. 3 Stupně zabezpečení dle ČSN EN 50141-1

Stupeň 1:	Nízké riziko (garáže, chaty, byty, rodinné domy, strojovny)
Stupeň 2:	Nízké až střední riziko (komerční objekty)
Stupeň 3:	Střední až vysoké riziko (ceniny, zbraně, informace, narkotika)
Stupeň 4:	Vysoké riziko (zejména objekty národního a vyššího významu)

Tab. 4 Doporučená ochrana

Ochrana objektu	Detekce	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
1. Vstupy-otevření	Kontakt	Ano	Ano	Ano	Ano
2. Vstupy-průnik	Prostorový detektor	Vhodné	Vhodné	Ano	Ano
3. Vstupy-uzamčení	El. zámek	Ne	Ne	Vhodné	Ano
4. Chodby prostor	Prostorový detektor	Ano	Ano	Ano	Ano
5. Otevření oken	Kontakt	Ne	Ano	Ano	Ano
6. Průraz oken	Akustické čidlo	Ne	Ano	Ano	Ano
7. Prostor místnosti	Prostorový detektor	Vhodné	Přednostně	Ano	Ano
8. Stěny stropy podlahy	Vibrační apod.	Ne	Ne	Volba	ano
Signalizace poplachu					
1. Vnitřní siréna		Ano	Ano	Ano	Ano
2. Venkovní siréna		Ano	Ano + volba	Ano + volba	volba
3. Telefonní zpráva		Doporuč.	Volba	Volba	Volba
4. Telefonní PCO		Volba	Doporuč.	Ano+volba	Ano + volba
5. RST přenos PCO		Volba	Doporuč.	Ano + volba	Ano + volba
6. Fyzická ostraha		Ne	Ne	Volba	Ano + volba
7. Přivolání pomoci		Ano při b.3,4	Doporuč.	Ano	Ano

4.4 Způsoby ochrany přepážkových pracovišť

4.4.1 Tísňová signalizace

Tísňovou signalizací je součástí elektronického zabezpečovacího systému. Jsou v činnosti v pracovní době většinou na všech přepážkách. Mimo pracovní nebo provozní dobu je po uzavření systému v činnosti plášťová a prostorová ochrana objektu. Tísňové hlásiče jsou

instalovány do prostor, kde se provádí manipulace s hotovostí. Jedná se o prostory, kde jsou prováděny dotace nebo odvody peněz, počítání hotovostí a následné další zpracování. Patří sem hlavní pokladny umístěné v zázemí pobočky, komorové trezory, bezpečnostní schránky, dotační boxy, bankomaty atd.

Při rozmísťování tísňových hlásičů musí být brán ohled na celkový počet zaměstnanců, jejich rozmístění, zabezpečuje prostory, odkud se zaměstnanci při napadení nemohou sami dostat, jsou například v této místnosti uzamčeni. Při výběru a umístění tísňového hlásiče musíme brát také v úvahu nestandardní situace, kdy může být zaměstnanec svázán. Možnost spuštění poplachu například nohou, popřípadě jinou částí těla, hlásiče musí být nainstalovány skrytě, tak aby nebyly viditelné z veřejného prostoru, ale umístěny tak, aby mohlo dojít k nepozorovanému a bezhlučnému spuštění poplachu. Pohyb ke spuštění poplachu musí být nacvičen, aby zaměstnanec tlačítko nehledal, ale spuštění poplachu bylo přirozené, plynulé a hlavně nenápadné.

Vhodné je i používání mobilních tísňových hlásičů, které má zaměstnanec v podobě malé krabičky nebo klíčenky umístěny v kapse svého oděvu. Zde je důležitá kontrola, zda je zařízení na svém místě a spolehlivě připraveno.

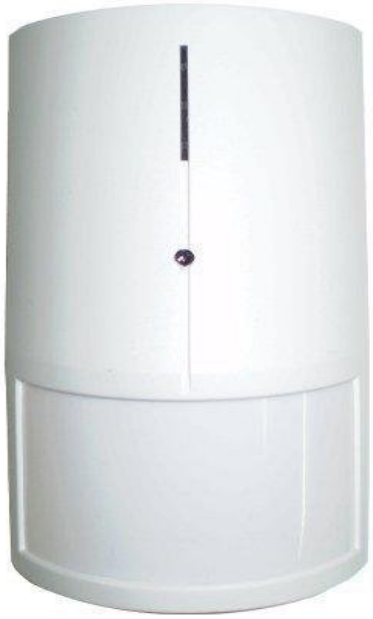
Další neméně důležitou úlohou při spuštění poplachu je předat tuto informaci nejenom na pult centralizované ochrany Policie ČR, ale také ostatním zaměstnancům. Je také důležitá zpětná vazba pro zaměstnance, že poplach byl spuštěn, ale musí být také upozorněni další zaměstnanci, že k přepadení došlo. Tím se zabrání, aby zaměstnanci z jiných prostor nevstoupili do místa přepadení, tím snížíme počet ohrožených osob. Informace může například probliknout na monitorech počítačů ve formě domluvené neutrální zprávy, nebo zaslání zprávy na mobilní telefon.

Při vyhlášení poplachu je vhodné, aby nedocházelo k viditelnému upozornění, že ke spuštění došlo. Velmi důležitým faktorem je řádné proškolení zaměstnanců a simulování možných situací přepadení s možností vyzkoušení vyhlášení poplachu.

Pokud není každý zaměstnanec na pobočce řádně proškolen, postrádá i ten nejmodernější systém smysl a vynaložené finanční prostředky jsou zbytečnou investicí.

4.4.2 Kamerové systémy

Kamerový systém je další součástí elektronického zabezpečovacího systému a zároveň důležitým prvkem ochrany přepážkových pracovišť. Výhodou je monitorování prostoru na pokladním místě, ale jejich umístění můžeme realizovat na jakémkoliv pro banku důležitém místě. Vhodné je umístění kamer ke vstupům do úřadoven banky. Kamerový systém nám umožňuje ověřit stav, který je signalizován například elektronickým zabezpečovacím nebo požárním systémem. Výhodou je, že záznam je ukládán na záznamové médium a lze použít při zpětném vyhodnocení situace, jako důkazový materiál k usvědčení pachatele při loupežném přepadení, popřípadě při jiné mimořádné události jakou je například podvodné jednání. Nahrávací zařízení kamerového systému musí být trvale zapnuto a nastaveno tak, aby byl nahráván obrazový záznam po dobu 24 hodin. Není vhodné zařízení vypínat, nebo jinak přerušovat. Je důležité, aby monitor byl ve stanovené pracovní době zapnutý. Nepovoleným osobám nesmí být umožněno sledovat obraz na monitoru. Obsluha systému musí také zajistit provádění úkonů v rozsahu daném výrobcem. Mezi tyto úkony patří prověřování funkčnosti zařízení, kontrola pořízených záznamů, udržování data a času, se kterým systém pracuje. Záznamové zařízení musí být také uloženo tak, aby nedošlo k jeho zneužití nebo odcizení. Nosiče respektive na nich uložené záznamy, obsahují bankovní tajemství podle zákona č. 21/1992 Sb., o bankách v platném znění a osobní údaje podle zákona č. 101/2000 Sb., o ochraně osobních údajů v platném znění.



Obr. 19 Maskovaná kamera v PIR Jablotron JS-20 [22]

4.4.3 Elektronický požární systém

Systém pracuje plně automaticky v režimu DEN/NOC. Hlavní úlohou EPS je pomocí akustického signálu upozornit na výskyt požáru a aktivovat poplach s výstupem na operační středisko hasičského záchranného sboru. Chování zaměstnanců v případě požárního poplachu musí být součástí školení zaměstnanců v oblasti požární ochrany.

Požární poplachová směrnice musí být trvale přístupná a viditelná pro všechny zaměstnance, kteří jsou trvale nebo přechodně určeni k výkonu pracovní činnosti v prostorách pobočky.

4.4.4 Fyzická ostraha

Fyzická ostraha nám slouží jako prevence a pomoc ke snížení rizika v pobočkách finančních institucí. V případě mimořádné události pracovníci ostrahy provádí neprodleně opatření ke zmírnění následků mimořádné události a zajišťují přivolání pomoci. Jedná se o důležitou část systému ochrany banky. Pracovníci fyzické ostrahy jsou viditelně označení jako bezpečnostní pracovníci a jsou oblečeni v uniformě. V současné době je fyzická ostraha řešena soukromými bezpečnostními agenturami a proto musí bankovní domy přesně definovat:

-způsob a místo vykonávání ostrahy, včetně vymezení prostor, kam mají pracovníci ostrahy přístup a za jakých podmínek

-musí vést dokumentaci o průběhu výkonu služby s přesně daným obsahem a způsobem jejího vedení

-výstroj a výzbroj pracovníků ostrahy

-práva a povinnosti pracovníků ostrahy

-požadavky na obsluhu technických zařízení

-způsob předávání informací o stavu střeženého objektu a určení kontaktní osoby

Záznam o průběhu služby identifikuje pracovníky ostrahy, kteří byli ve službě a po jakou dobu. Jsou zde zaznamenány informace o všech podstatných událostech, ke kterým v průběhu služby došlo. Jedná se hlavně o mimořádné události, zjištěné rizika. Komu byla rizika hlášena a co bylo podniknuto ke zmírnění nebo odvrácení zjištěných rizik. Dále zde mohou být uvedeny technické závady na zařízení objektu atd. Záznamy musí být vedeny tak aby nešly zpětně pozměnit. Pokud je nutné nějaký údaj doplnit, změnit musí být uveden důvod změny, datum a proč byl záznam upraven.

Soukromá bezpečnostní agentura odpovídá za to, zda službu vykonávají osoby, které splňují předpoklady osobní spolehlivosti, jsou bezúhonní a odborně způsobilé.

Oprávnění a povinnosti pracovníků ostrahy

- jsou povinni postupovat v souladu s obecně závaznými právními normami, zejména občanského zákoníku, trestního zákona, zákoníku práce a pravidly stanovenými pro výkon služby smlouvou uzavřenou mezi bezpečnostní agenturou a peněžním ústavem.
- proti narušitelům zájmů peněžních ústavů jsou oprávněni zakročit v případech nutné ochrany, krajní nouze § 13 a 14§ Trestního zákona nebo svépomoci § 6,§ 126,§ 417,§ 418 Občanského zákoníku. Dále pak mohou zadržet pachatele trestného činu za podmínek stanovených trestním řádem § 76 odst. 2
- na místě trestného činu si počínají tak, aby neztížili plnění úkolů orgánů činných v trestním řízení

- v případě napadení pobočky nesmí svým jednáním zvýšit nebezpečí fyzického útoku nebo i použití zbraně pachatelem vůči zaměstnancům, klientům jiným osobám.

Navrhuji používání střelné zbraně pouze v situacích, kde hrozí mimořádné riziko napadení příkladem ochrana přepravy hotovostí. V prostorách bank, které jsou volně přístupné veřejnosti, by služba pracovníky ostrahy měla být vykonávána bez střelné zbraně.

4.4.5 Režimová opatření banky

Z důvodu bezpečnosti objektů bank je velmi důležité rozčlenit objekt na jednotlivé zóny. Toto rozdělení nám pomáhá určit oprávněný přístup zaměstnancům a návštěvám objektu a co mohou v těchto prostorách vykonávat.

Vzhledem k přehlednosti navrhuji rozčlenit bankovní dům do 5 zóny. Vycházela jsem ze stavu nutných prostor, které obklopují banku a prostor, které banky potřebují ke své činnosti. Při rozdělení na více zón pak může docházet k nepřehlednosti a nedodržování pravidel.

Zónu 1 – jsem označila jako veřejnou. Do této zóny patří venkovní komunikace a parkoviště, vstupní prostory a vnitřní komunikace, bankovní haly, samoobslužné zóny, prostory před bankomaty, nočními trezory. Tato zóna je částečně vně a částečně zasahuje do vnitřních částí budovy a je ohraničena stavebními konstrukcemi uvedených prostor. Vstup a pohyb v této zóně je omezen pouze fyzickými překážkami, pokud jsou v objektu umístěny a informačními tabulemi.

Zóna 2 – v této zóně jsou již pouze vnitřní části objektu, mohou to být pomocné plochy, jako jsou recepce, vestibul, jídelna, bufet. Vstup a pohyb v této zóně je určen příslušným oprávněním např. průkazem zaměstnance, je zde možný i samostatný pohyb cizích osob a návštěv.

Zóna 3 – jedná se o vnitřní prostory budovy, jako jsou kanceláře, zasedací místnosti, vnitřní komunikace, personální výtahy. Vstup a pohyb v této zóně je určen příslušným oprávněním, průkazem zaměstnance. Pohyb cizích osob a návštěv je možný pouze s doprovodem nebo přítomností určených zaměstnanců.

Zóna 4 – jedná se o vnitřní prostory budovy s vyšší úrovní bezpečnosti např. zázemí poboček, zvláště pokladních míst, účtárny, spisovny, archivy, kanceláře IT, technické místnosti a plochy pro podpůrné systémy jako je UPS, rozvodny, strojovny, kotelny, vnitřní parkoviště, stravovací provoz, nákladní rampy. Vstup a pohyb v této zóně je určen příslušným oprávněním, průkazem zaměstnance a v některých případech jsou nutné přístupy v EZS. Vstup a pohyb návštěv je zakázán, pod dohledem učených zaměstnanců je vstup možný pracovníkům smluvních dodavatelů.

Zóna 5 – to se již jedná o vnitřní prostory budovy, které jsou zastoupeny místnostmi vysoké úrovně bezpečnosti, patří sem telefonní ústředny, datové uzly v objektu, serverové místnosti, IT sály, trezory, místnosti ATM, hlavní pokladny, dotační boxy a místnosti, místnosti se zabezpečovací technikou. V této zóně se mohou pohybovat pouze oprávněné osoby, tj. určení zaměstnanci a určení zaměstnanci smluvních dodavatelů, který jsou v doprovodu a za stálé přítomnosti určených zaměstnanců.

-Podmínky pro vstup osob do zóny 1 až 3 v pracovní době:

- Do zóny 1 je vstup povolen neomezeně a bez evidence, kromě osob budící veřejné pohoršení nebo osoby, které by svým chováním ohrožovaly bezpečnost osob nebo majetku. Jedná se o osoby pod vlivem návykové látky, obtěžující klienty nebo zaměstnance. Stejná pravidla platí i pro zónu 2.
- Do zóny 3 mohou vstupovat klienti v otevírací době, jedná se o klienty, se kterými není z oprávněných důvodů možné jednat nebo není vhodné bankovní operace realizovat na přepážkách nebo otevřených pracovištích. Do prostoru jsou vpuštěny za předpokladu, že řádné identifikace a jsou přímými účastníky bankovní operace. Pokud je nutný pohyb v jiném prostoru banky musí být vždy za doprovodu zaměstnance. V knize návštěv se vede evidence návštěv a dodavatelů nebo servisních firem.

-Podmínky pro vstup osob do zóny 4 v pracovní době

- Vstup do těchto prostor je povolen pouze zaměstnancům určeným vedoucím zaměstnancem pobočky, útvaru, oddělení za účelem plnění pracovních povinností. Jedná se např. o vstupy do archívů.

-Podmínky pro vstup osob v mimopracovní době nebo ve dnech pracovního klidu a ve svátek

- Volný vstup do vnitřních prostor zařazených v jednotlivých zónách je povolen pouze zaměstnancům pracovně zařazeným v objektu, kteří se dostaví za účelem řešení mimořádných událostí. Jedná se o situace při poplachu nebo poruše EZS, při napadení objektu, požáru. Povolen vstup je také zasahujícím příslušníkům Policie ČR, Hasičskému záchrannému sboru a pracovníkům zdravotnické záchranné služby. Ostatním zaměstnancům, zaměstnancům dodavatelských firem a dalším přesně určeným osobám je vstup povolen pouze po předložení zvláštního povolení uděleného vedoucím zaměstnancem, toto nemusí platit při řešení mimořádných situací, u kterých hrozí nebezpečí z prodlení např. napadení objektu, oprava EZS, technická závada zařízení budovy. Tyto osoby budou vždy v doprovodu určeného zaměstnance. Vstup do prostor zařazených do zóny 4 a 5 v mimopracovní době je povolen pouze ve výjimečných případech a to vždy s písemným souhlasem ředitele pobočky, jedná se zejména o komorové trezory nebo trezorové místnosti.

-Úklid objektu – většinou je úklid objektu zajištěn dodavatelsky, z tohoto důvodu popisuji režim vstupu do objektu, do kterého budou vpuštěni pouze zaměstnanci úklidové firmy, uvedení na zvláštním seznamu, který musí být při každé změně včas aktualizován. Zaměstnanci, kteří nejsou v seznamu, nesmí být do objektu vpuštěni. Úklid prostorů by měl být prováděn v pracovní dny v dohodnuté době, ale mimo otevírací dobu pobočky. Úklid, který se bude provádět v zónách 4 a 5 je možný pouze v přítomnosti zaměstnanců přímo odpovědných za uložené hodnoty nebo instalovaných zařízení.

Sami zaměstnanci musí dodržovat bezpečnostní pravidla provozu pobočky. Musí důsledně dodržovat uzamykání mechanických zábran, oddělující jednotlivé zóny. Na svém pracovišti jsou odpovědni za zabezpečení jim svěřených písemností, cenností a pracovních pomůcek, u kterých lze předpokládat jejich zneužití nebo odcizení.

5 NÁVRH NA SNÍŽENÍ BEZPEČNOSTNÍCH RIZIK

Ani sebelepší zabezpečovací technikou nedosáhneme požadovaného výsledku, pokud do bezpečnostního systému nezapojíme samotné zaměstnance poboček finančních institucí. Je důležité si uvědomit, že vzhledem k jejich pracovní náplni, vytíženosti a ve většině případů netechnické profesi, není v silách zaměstnanců zapamatovat si mnohdy jednoduché kroky při obsluze EZS, EPS atd. Je ovšem na místě, aby zaměstnanci pracující v prostředí s možným výskytem bezpečnostních rizik spolehlivě tuto zabezpečovací techniku ovládali, znali funkce a umístění jednotlivých prvků na svém pracovišti, musí také provádět pravidelnou kontrolu funkčnosti zařízení. Situace může být stejná i v případě mimořádných událostí, které mnohdy nastávají v delším časovém horizontu, kdy jednotlivé kroky a postupy jednoduše zapomenou. Proto je důležité, kromě povinných školení, mít také vypracovány postupy a doporučení, jak se v určitých situacích zachovat. Dalším nejdůležitějším krokem ke snížení bezpečnostních rizik by mělo být samozřejmostí zachovávat mlčenlivost o způsobu zabezpečení objektu a jeho provozu před nepovolanými osobami.

5.1 Bezpečnostní zásady na snížení bezpečnostních rizik

5.1.1 Vstup a odchod z pobočky

- Dle možností a podmínek měnit trasy příchodu a odchodu k pobočce.
- Sledovat pohyb a přítomnost podezřelých osob v blízkosti pobočky.
- Před odchodem z pracoviště se přesvědčit o situaci před vchodem do pobočky. V případě jakéhokoliv podezření neopouštět pobočku a vyrozumět Policii ČR.

Tyto jsou zásadní. Pokud chce lupič přepadnout pobočku zneužitím zaměstnance, nejdříve musí vysledovat a mapovat okolí pobočky. Může dokonce zaměstnance sledovat, až do místa jeho bydliště. Dále sleduje počet osob, které jsou při otevírání a uzamykání pobočky.

Doporučení: minimálně dva zaměstnanci musí být přítomni při odemykání a uzamykání pobočky. Přitom pokud to situace dovolí postupovat tak, aby nebylo zřejmé, kdo má v držení klíče od pobočky. Dále si domluvit signál, který je použit, pokud dojde k zneužití, nebo nátlaku na zaměstnance. Osvědčeným signálem je začít si tykat, pokud si zaměstnanci vykají a naopak.

- Před odemknutím pobočky si ověřit neporušenost vstupních dveří, zámků a mříží.
- Po příchodu na pracoviště zkontrolovat neporušenost vnitřního prostoru pobočky, úschovných objektů, zabezpečovací techniky, telefonní linky, zda nebylo manipulováno s uloženými věcmi, nebylo poškozeno vybavení pobočky.
- Zadní vchody musí být hned po použití znovu uzamčeny a musí být provedena kontrola správného uzamčení.

5.1.2 V pracovní době pobočky

- Je důležité věnovat pozornost osobám, které navštěvují pobočky opakovaně, bez zjevného důvodu. Snažit se oslovit tyto osoby k účelu jejich návštěvy. Zvýšit pozornost vůči osobám, které navštěvují pobočku častěji nebo opakovaně v krátkém časovém intervalu jako klienti. Může se jednat o tzv. tipaře.
- Je nezbytné věnovat zvýšenou pozornost osobám, které v prostorách banky používají mobilní telefony, jedná se o bezpečnostní riziko ve vztahu k zajištění bezpečnosti prováděných operací a poskytování bankovních služeb klientů.
- Všechny vedlejší vchody do pobočky musí být uzamčeny. Je důležité si uvědomit, že klíče neponecháváme v žádných dveřích pobočky. Může dojít k jejich odcizení, vyrobení duplikátu, odemknutí dveří pro následnou přípravu vniknutí do pobočky. Zaměstnanci mohou být i v, kde je ponechán klíč v zámku, pachatelem uzamčeni.
- Pokladníci mohou do svých pokladen z trezorů vkládat pouze hotovost, která je jim stanovena pokladním limitem. Hotovost nad tento limit, musí být uložena do trezorů. Trezory neboli úschovná zařízení jsou po celou pracovní dobu uzamčeny. Toto pravidlo platí i pro pokladní místa, která jsou opatřena skleněnou nadstavbou a dveřmi.
- Při opuštění pracoviště je nutné uzamknout peněžní hotovost, pokud nelze hotovost bezpečně zajistit je nutné ji uložit do úschovného objektu.
- Pokud to situace umožňuje příležitostně sledovat situaci v blízkosti pobočky např. zaparkovaných vozidel jeho osádky.
- Po ukončení pracovní doby, před odchodem z pracoviště musí zaměstnanci uzavřít všechny okna, vypnout elektrické spotřebiče (především rychlovarné konvice, kávovary a jiná zařízení, která mohou bez dozoru nebo při závadě způsobit požár. Je nutné mít u těchto zařízení vyvěšeny informace o vyjmutí ze zásuvky a jméno osoby, která je za tento stav odpovědná), dále uzamknout dveře a mříže.

- Písemnosti musí být zajištěny tak, aby nedošlo k jejich poškození, zničení nebo ztrátě. Spisový materiál, který je předmětem bankovního tajemství musí být zajištěn proti zneužití třetí osobou.
- Před uzamčením hlavního vchodu do pobočky sledovat situaci v prostoru pro klienty, není bezpečné doprovázet posledního klienta. Po uzamčení hlavního vchodu již žádné osoby do pobočky nevpouštět pod jakoukoliv záminkou. Je důležitá kontrola veřejných prostor pro klienty, zda zde není zapomenut podezřelý předmět, nainstalováno zařízení nepatřící do inventáře pobočky, úmyslně poškozeno zařízení pobočky. Také je nutné provést kontrolu všech vhazovacích schránek, které se nachází v prostorách pro klienty. Mohou to být schránky, kde klienti vhazují náměty a připomínky, nebo to mohou být sběrná zařízení např. na příkazy k úhradě.

5.1.3 Chování zaměstnanců při loupežném přepadení

Tímto postupem chci snížit bezpečnostní riziko, při loupežném přepadení pobočky banky. Hlavní úlohou tohoto postupu je uklidnit zaměstnance, který se při loupeži cítí ohrožen a je pod psychickým tlakem a chci dosáhnout, aby nebyl v žádném případě zbytečně zmařen lidský život. Návod má také zaměstnancům pomoc, jaké první kroky mají následovat krátce po útočníkově opuštění pobočky.

- Setrvejte v poloze, v jaké Vás situace zastihla. Důležité je nepodlehnout šoku, začněte pomalu a zhluboka dýchat, dělejte pomalé pohyby, jsou to kroky, které Vás pomalu uklidní. Vaše klidné jednání se zpravidla přenese i na pachatele naopak projevy nervozity, nekontrolované, neklidné pohyby pomohou způsobit opak.
- Plňte pokyny pachatele, nedělejte nic, co by mohlo vyvolat jeho negativní, násilnou reakci a tím i ohrožení Vaše nebo jiných osob.
- Pokud jste vystaveni jednání pod nátlakem, domluvte si se svým okolím např. spolupracovníkem, rodinným příslušníkem určité heslo, je možné, že Vám náhodou zavolají nebo se mohou objevit na pobočce. Objasněte tyto osoby, jak se mají zachovat při jeho použití.
- Tísňový hlásič použijte pouze v případě, že jeho použití nemůže být pachatelem zpozorováno. Pokud použijete výklopný tísňový hlásič, pokuste se výklopnou část

vrátit do původní polohy, znemožní se identifikace osoby, která poplach vyvolala a sníží se tak Vaše ohrožení.

- Pokud možno se vyhněte fyzickému kontaktu s pachatelem. Je-li to možné sledujte s určitým odstupem únikovou cestu, důvodem je zjištění směru úniku, možného spolupachatele, použití dopravního prostředku a směru odjezdu. Pokud jsou na místě svědci, upozorněte je na situaci přepadení.
- Poskytněte první pomoc zraněným nebo spoutaným osobám, pokud to vyžaduje situace, přivolejte lékaře.
- Lékařskou pomoc přivolejte i v případě, pokud je některý ze zaměstnanců v nervovém šoku.
- Uzamkněte vstupní dveře do pobočky a ihned, pokud nebyl vyvolán poplach, informujte Policii ČR.
- Další informace o přepadení by mělo obdržet vedení banky a bezpečnostní specialista
- Je důležité nechat vše na místě činu v původním stavu. Nedotýkejte se míst, kterých se dotýkal pachatel, i když měl rukavice. Zabraňte komukoliv, s výjimkou osob poskytující první pomoc, ve vstupu na místo činu. V žádném případě na místě činu nekuřte.
- V případě, že nebyla odcizena celá peněžní hotovost, uložte bezpečně zbylou částku.
- Svědky události požádejte o vyčkání do příjezdu Policie ČR. Zůstávejte v místech, kde se nepohyboval pachatel. Pokud tyto osoby nemohou setrvat na místě, dle občanského průkazu požádejte o osobní údaje.
- Vyberte zaměstnance, který bude u vchodu vyčkávat policii a po jejím příjezdu podá nezbytné informace o situaci na pobočce
- Je důležité neprobírat vzniklou situaci se svědky ani se zaměstnanci, důvodem je, aby nedocházelo k ovlivňování Vašich vjemů.

5.1.4 Další návrhy na snížení rizik

Největším přínosem na snížení bezpečnostních rizik je správné používání EZS a zásadní je tento systém používat i během dne. Jedná se hlavně o používání střežení trezoru v průběhu pracovní doby. Mnohým zaměstnancům se tento úkon zdá zbytečný, když je trezor ještě uzamčen klíčem, ale při přepadení pobočky, může zaměstnanec otevřít trezor a při

zastřežení spustí poplach a tím přivolá pomoc. Není možnost vyvolání poplachu, pokud není ještě tísňové tlačítko nainstalováno v trezoru, nebo pokud zaměstnanec nemá tísňový hlásič u sebe.

5.1.5 Návrhy na ochranu bankomatů před neoprávněnými výběry

Nejúčinnější ochranou pro zamezení kopírování karet je zavedení pouze čipových karet. Přechod na čipovou technologii, by mohl znamenat snížení skimmingu, ale v současné době je již vyvinuto zařízení na kopírování těchto platebních karet. Podvodníci tohoto zařízení nevyužívají. Důvodem je finanční stránka, karty s čipem spolu s kopírovacím zařízením jsou mnohonásobně dražší, než je tomu při pořizování zařízení pro skimming magnetických karet. Dále je nasazení karet z globálního hlediska nemožné. Muselo by dojít k úpravě většiny bankomatů, protože není samozřejmostí, že všechny bankomaty jsou vybaveny čipovou technologií, která zpracovává informace pouze z čipu karty. V České republice začínají banky vydávat tzv. hybridní platební karty. To znamená, že platební karta obsahuje jak magnetický proužek, tak čip. Tento krok, ale neřeší kopírování magnetických karet, je to pouze malý krok k přechodu na čipové karty. Proto banky musí nadále investovat finanční prostředky na zamezení kopírování platebních karet.

Mohu doporučit velmi účinný prostředek k zamezení nainstalování skimmingového zařízení na otvor pro platební karty. Jedná se o jednoduchou instalaci zeleného poloprůhledného plastu s integrovaným hologramem. Zvolením průhledného plastu, který je ještě navíc přerušovaně prosvěcován indikátorem čtečky je vidět přítomnost cizího zařízení, což značně omezuje kopírování platebních karet.

Také pomocí softwarové úpravy se karta při vstupu do bankomatu pohybuje trhavě nebo přerušovaně a právě tento pohyb eliminuje možnost podvodně načíst údaje z magnetického proužku.

Obr. 20 Anti-skimmovací nástavec [20]

Pro klienty je napsáno mnoho návrhů a doporučení, jak se chovat při výběru hotovosti u bankomatu. Nebudu zde proto vymýšlet jiný návod, který by ve své podstatě kopíroval, co již bylo vymyšleno a napsáno. Ale vzhledem k tomu, že se snažím touto kapitolou podat návrhy na snížení bezpečnostních rizik, je na místě, zde tento postup chování uvést. K tomu jsem využila návodu, který navrhuje Policie ČR, který je dostupný na stránkách www.policie.cz/clanek/skimming-2011.aspx.

Vaše platební karta a vaše finanční prostředky na účtu budou lépe ochráněny proti zneužití pokud:

- *budete mít svou kartu neustále pod dohledem;*
- *uchováte PIN kód v naprosté tajnosti (nesdělovat jiné osobě, nezaznamenávat v mobilním telefonu, na kartě, v dokladech apod.);*
- *při výběru z bankomatu věnujete zvýšenou pozornost místu, kde výběr provádíte (zaměřte se na nejbližší okolí a pohybující se osoby, důkladně si bankomat prohlédněte, zda na něm nejsou provedeny konstrukční změny a úpravy);*
- *pro výběr finančních prostředků z bankomatu volte raději frekventované a dostatečně osvětlené místo,*

- *při zadávání číselné kombinace PIN kódu na klávesnici zakryjete část základní desky s čísly druhou rukou (tímto způsobem můžete zabránit možnému odpozorování číselné kombinace);*
- *při transakci neztratíte kontrolu nad kartou a nenecháte se nikým a ničím ovlivnit;*
- *transakci neuskutečníte při podezření, že něco není v pořádku;*
- *vždy kontrolujete výpisy transakcí proti prodejním a výplatním dokladům (sledujete tak možný výskyt neoprávněných transakcí);*
- *při podezření, že je na bankomatu umístěno skimmovací zařízení, neprodleně informujete Policii ČR prostřednictvím linky 158 nebo 211, popřípadě bankovní společnost (kontaktní infolinka bývá na bankomatech umístěna),*
- *při platbě kartou v restauraci či prodejně dbejte, aby platební transakce proběhla pod vaším dohledem (personál by neměl kartu nikam odnášet),*
- *při platbě kartou na internetu si předem ověřte důvěryhodnost serveru.(literatura)*

Existuje elektronické zařízení, které je instalováno do vnitřní části bankomatu. Jedná se o zařízení názvem ADT Anti – Skim, které nabízí americká firma ADT. Jedná se o přístroj, který poskytuje bankomatu vícenásobnou ochranu proti skimmingu. Vytváří ochranný štít okolo vstupního otvoru pro platební karty, který pomáhá zjistit skimmovací zařízení a zároveň chrání data uživatele bankomatu. Přitom není narušena komunikace bankomatu po síti. Povrchový senzor detekuje cizí objekty před čtečkou karet a vyvolá alarm, přitom se nepřeruší platební transakce klienta. Mezi tím je k postiženému místu vyslána Policie, která může přichytit pachatele přímo při následné deaktivaci zařízení. Zařízení nevyžaduje žádné specifické úpravy softwaru.

Jádrem řešení ADT Anti-Skim je zařízení, které vysílá elektomagnetické pole, které ruší činnost illegálních kartových čteček bez toho, aby byla dotčena platební transakce řádného uživatele bankomatu a dále Surface Detection Kit (SDK) - senzor, který pomáhá detekovat neodpovídající zařízení na vstupním otvoru pro platební karty, přičemž lze detekovat předměty zhotovené z různého materiálu (plastu, papíru, kovu, dřeva..). Detekce objevu vnějšího předmětu spouští příslušný alarm. Vzhledem k vícenásobným výhodám, které toto zařízení má, není v České republice používáno.

Obr.21 Umístění ADT Anti-Skim [23]

ZÁVĚR

Cílem diplomové práce bylo navrhnout opatření, které by snížilo bezpečnostní rizika na přepážkách bankovních domů. Ve své práci jsem se zaměřila na chování zaměstnanců a jejich každodenní úkony, které provádějí při příchodu a odchodu z pracoviště. Zaměstnanci většinou podceňují rizika, které mohou ovlivnit svým chováním. Ve své práci jsem se snažila pro zaměstnance vypracovat postupy chování při příchodu a odchodu z pobočky. Snažila jsem se zdůraznit správné používání zabezpečovací techniky a dodržování režimových opatření, poněvadž banka do tohoto zabezpečovacího systému vkládá nemalé finanční prostředky a také je nutno dodržovat požadavky pojišťoven. Jenom funkční kamerový systém, který zaznamenal průběh přepadení, může být důkazem a předmětem pro rychlé odhalení pachatele.

Dále jsem pro zaměstnance vypracovala postupné kroky chování, které mohou použít při loupežnému přepadení pobočky, tak aby byli schopni po přepadení zajistit místo činu a byli schopni podat Policii kvalitní informace.

Dále jsem se snažila navrhnout opatření, které by eliminovalo bezpečnostní rizika při výběru hotovostí z bankomatů. V současné době jsou největšími podvody na bankomatech kopírovací zařízení magnetických karet. Ve své práci jsem doporučila zařízení, které by výskyt tohoto druhu podvodu mohl snížit a také úplně zastavit. V každém případě bych bankám doporučila používat zařízení ADT Anti-Skim, které by mohlo dopadnout pachatele přímo na místě činu. Jak jsem již zmínila, toto zařízení se v České republice nepoužívá. Používají se levnější varianty, které znemožňují nasazení kopírovacího zařízení na otvory pro vstup platební karty, ale i s tímto problémem se pachatelé dovedou v dnešní době vypořádat v podobě napodobenin celých panelů bankomatů. Dalším řešením pro zabránění kopírování karet je menší softwarová úprava, jejíž podstatou je trhavé zajíždění platební karty do bankomatu. Těmito nepravidelnými pohyby se zabrání kopírovacímu zařízení plynulé načtení karty, vzhledem k tomu, že toto kopírovací zařízení je na povrchu otvoru pro platební karty.

Do budoucna lze předpokládat nárůst těchto podvodů i vzhledem k tomu, jak se banky snaží na svých pobočkách zabezpečit peněžní hotovost, snižovat limity hotovostí na pobočkách a nejvíce podporují bezhotovostní transakce a využívají různé techniky znehodnocení ukradené hotovosti.

Pokud bych měla navrhnout řešení, které by zabránilo kopírování karet, bezesporu by to byl návrh na přechod pouze na čipovou technologii. Hotovost by byla vybírána bezkontaktním způsobem pomocí čtecího zařízení na bankomatu. Karta by neprocházela žádným otvorem, aby nemohlo dojít ke kopírování údajů na kartě.

ZÁVĚR V ANGLIČTINĚ

The goal of the thesis was to propose arrangements which would decrease a security risk on the bank cash desks. In my thesis I focused on the bank staffs behavior and their operation tasks, which they process during entering and leaving the bank building. The bank staffs usually underestimate the risks which can be influenced by their behavior. I have tried to prepare some procedures which the Staffs should respect during entering and leaving the Bank building. I highlighted the proper usage of the safety appliance and adherence to the rules because Banks invest huge amount of money into this appliances. Furthermore Insurance companies require proper appliance usage to be fulfilled insurance contracts. Only proper working DVR security system, which recorded an aggression can serve as an evidence for a fast capture of criminals.

Additionally I prepared for the Staffs a process which they can use in case of an aggression to secure of locus delicti and ti be able to inform the Police in a right way.

A next area which I focused on was eliminating of security risks with ATM customer working (cash withdrawals). Today problems of ATM are frauds made via an illegally installed card readers. In my thesis I recommended a device which could reduce or eliminate the frauds. Definitely I would recommend to the Banks to use the device ADT Anti-Skim which allow to catch criminals on locus delicti. The Device is still not use in the Czech Republic. There are used cheaper variants, which should prevent to install illegal card readers on the ATM card entrance but criminal have a workaround, where are installed a whole illegal dummy ATM panels. A next solution, which mitigate criminals ATM attempts, is a software modification which deliver customer cards into ATM with the jerky movement preventing a possible illegal reader to read data.

In the future can be expected increasing number of criminal attempts to get a cash so the Banks secure themselves e.g. by decreasing of cash in the Bank buildings, supporting credit transfers and implementation of various techniques which depreciate paper money when they are stolen.

If I would to propose a solution which would prevent the illegal customer card copying then it would be a proposal to implement only Chip cards. Cash would be withdrawn by non contact technology via an appropriate ATM reader. Cards would not need to be passed via any gate and by this would vanish a thread of card copying.

SEZNAM POUŽITÉ LITERATURY

[1] ČERNÝ,J., IVANKA,J., Systematizace bezpečnostního průmyslu I. 2 vydání. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006. 135 s. ISBN 80-7318-402-8

[2] SMEJKAL, V., RAIS, K., Řízení rizik ve firmách a jiných organizacích. 2.vydání. Praha: Grada Publishing, a.s., 2006. 296 s. ISBN 80-247-1667-4

[3] KINDL, J., Projektování bezpečnostních systémů I. 2. vydání. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007. 134 s. ISBN 978-80-7318-554-1

[4] TICHÝ, M., Ovládání rizika. Analýza a management. 1. vydání. Praha: C.H.Beck, 2006. 396 s. ISBN 80-7179-415-5

[5] LUDVÍK, M., ŠTEDROŇ. B.,Teorie bezpečnosti počítačových sítí. Praha: Computer media, 2008. 98 s. ISBN 978-80-86686-35-6

[6] KOCMAN, R., LOHNISKÝ,J., Jak se bránit virům, spamu a spyware. 1. vydání. Brno: CP Books, a.s. 2005. 148 s. ISNB 80-2510793-0

[7] JAŠEK, R., Informační a datová bezpečnost.1. vydání. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006. ISBN 80-7318-456-7

[8] LAUCKÝ, V., Technologie komerční bezpečnosti I. 3. vydání. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010. ISBN 978-80-7318-889-4

[9] STREBE, M., PERKINS, CH., Firewally a proxy-servery. 1. vydání. Brno: Computer Press, 2003. 450 s. ISBN 80-7226-983-6

[10] SZOR, P., Počítačové viry – analýza útoku a obrana. 1. vydání. Brno: ZONER software s.r.o., 2006. 608 s. ISBN 80-86815-04-8

[11] NEČAS, S. SEILER, M. a kolektiv. Loupežná přepadení pracovišť s peněžním provozem a jejich bezpečnost, 1. vydání, Praha 2004, Policejní akademie ČR, 262 s.

[12] Norma ČSN EN 50 131

[13] RAK, R., MATYÁŠ, V., ŘÍHA Z., Biometrie a identita člověka ve forenzních a komerčních aplikacích. 1. vydání. Praha: Grada Publishing, a.s., 2008, 664 s. ISBN 978-80-247-2365-5.

Elektronické zdroje:

[14] www.jablotron.cz

[15] http://www.ipcameras.cz/index.php/ipkamery/46-analogvsdigital

[16] www.pcporadenstvi.cz

[17] www.securityrevue.com

[18] http://pc.itek.cz/rackove-skrine-datove-rozvadece-rozvadece

[19] Ministerstvo vnitra ČR: [online]. [cit. 2012-03-05]. Dostupný z WWW: http://aplikace.mvcr.cz/archiv2008/hasici/planovani/metodiky/mzprakp.pdf

[20] Policie ČR: [online]. [cit. 2012-04-20]. Dostupný z WWW: http://www.policie.cz/clanek/skimming-2011.aspx

[21] Chip :Zmanipulované bankomaty : [online]. [cit.2012-04-20]. Dostupný z WWW: http://earchiv.chip.cz/cs/earchiv/vydani/r-2011/chip-01-2011/zmanipulovane-bankomaty.html

[22] www.a1com.cz

[23] ADT: anti-skim [online]. [cit. 2012-04-02]. Dostupný z WWW: http://www.adt.com/commercial-security/products/anti-skim-solutions/)

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ATM	Automatic Teller Machine
CCTV	Uzavřený televizní okruh
ČSN	Česká státní norma
EPS	Elektronická požární signalizace
EZS	Elektronický zabezpečovací systém
FTP	File Transfer Protocol
HW	Hardware
HZS	Hasičský záchranný sbor
IP	Internet Protokol
IS	Informační systém
I&HAS	Poplachové zabezpečovací a tísňové systémy
LED	Light Emitting Diode
MZS	Mechanické zábranné systémy
PC	Osobní počítač
PCO	Pult Centralizované Ochrany
PIN	Osobní identifikační číslo (Personal Identification Number
PIR	Passive infrared sensor
PZS	Poplachový zabezpečovací systém
SBS	Soukromá bezpečnostní služba
SW	Software
UPS	Uninterrupted Power Supply

SEZNAM OBRÁZKŮ

SEZNAM TABULEK