

Vysoká škola logistiky o.p.s.

**Logistika bezpečnostních procesů
a technologií spojených s monitoringem
chování zákazníků obchodu**

(Diplomová práce)



Vysoká škola
logistiky
o.p.s.

Zadání diplomové práce

student **Bc. Dušan Kalup**
studijní program Logistika

Vedoucí Katedry magisterského studia Vám ve smyslu čl. 22 Studijního a zkušebního řádu Vysoké školy logistiky o.p.s. pro studium v navazujícím magisterském studijním programu určuje tuto diplomovou práci:

Název tématu: **Logistika bezpečnostních procesů a technologií spojených s monitoringem chování zákazníků obchodu**

Cíl práce:

S využitím poznatků z bezpečnostních procesů a technologií analyzovat a profilovat podezřelé chování zákazníků obchodu. Získané informace využít pro nastavení bezpečnostních procesů obchodu za účelem zefektivnění monitoringu podezřelých osob.

Zásady pro vypracování:

Využijte teoretických východisek oboru logistika. Čerpejte z literatury doporučené vedoucím práce a při zpracování práce postupujte v souladu s pokyny VŠLG a doporučeními vedoucího práce. Části práce využívající neveřejné informace uveďte v samostatné příloze.

Diplomovou práci zpracujte v těchto bodech:

Úvod

1. Teoretická východiska problematiky monitoringu chování zákazníků
2. Monitoring osob ve specifickém prostředí obchodu
3. Návrh zefektivnění bezpečnostních procesů a technologií monitoringu
4. Vyhodnocení přínosů návrhu

Závěr

Rozsah práce: 55 – 70 normostran textu

Seznam odborné literatury:

DOUCEK, Petr a kol. Řízení bezpečnosti informací: 2. rozšířené vydání o BCM. Praha:Professional Publishing, 2011. ISBN 978-80-7431-050-8.

JAŠEK, Roman a David MALANÍK. Bezpečnost informačních systémů. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013. ISBN 9788074543128. Dostupné také z: <http://hdl.handle.net/10563/25821>.

KŘUPKA, Jiří a Miloš VÍTEK. Systémové inženýrství a informatika. Pardubice: Univerzita Pardubice, 2013. ISBN 978-80-7395-732-2.

LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management. Zlín: Radim Bačuvčík - VeRBuM, 2015. ISBN 9788087500675.

Kodexy chování: Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob [online]. Praha: Úřad pro ochranu osobních údajů, 2013 [cit. 2021-10-28]. Dostupné z: <https://www.uoou.cz/kodexy-chovani/d-29493/p1=3453>.

Vedoucí diplomové práce:

prof. Mgr. Roman Jašek, Ph.D., DBA


Datum zadání diplomové práce:

31. 10. 2021

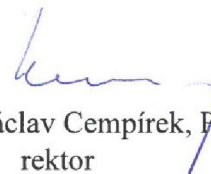
Datum odevzdání diplomové práce:

12. 5. 2022

Přerov 31. 10. 2021



Ing. Blanka Kalupová, Ph.D.
vedoucí katedry



prof. Ing. Václav Cempírek, Ph.D.
rektor

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a že jsem ji vypracoval samostatně. Prohlašuji, že citace použitých pramenů je úplná a že jsem v práci neporušil autorská práva ve smyslu zákona č. 121/2000 Sb., o autorském právu, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

Prohlašuji, že jsem byl také seznámen s tím, že se na mou diplomovou práci plně vztahuje zákon č. 121/2000 Sb., o právu autorském, právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména § 60 – školní dílo. Beru na vědomí, že Vysoká škola logistiky o.p.s. nezasahuje do mých autorských práv užitím mé diplomové práce pro pedagogické, vědecké a prezentační účely školy. Užiji-li svou diplomovou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat o této skutečnosti Vysokou školu logistiky o.p.s.

Prohlašuji, že jsem byl poučen o tom, že diplomová práce je veřejná ve smyslu zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, zejména § 47b. Taktéž dávám souhlas Vysoké škole logistiky o.p.s. ke zpřístupnění mnou zpracované diplomové práce v její tištěné i elektronické verzi. Tímto prohlášením souhlasím s případným použitím této práce Vysokou školou logistiky o.p.s. pro pedagogické, vědecké a prezentační účely.

Prohlašuji, že odevzdaná tištěná verze diplomové práce, elektronická verze na odevzdaném optickém médiu a verze nahraná do informačního systému jsou totožné.

V Přerově, dne 12. 05. 2022

.....

podpis

Poděkování

Rád bych poděkoval panu prof. Mgr. Romanu Jaškovi, Ph.D., DBA za vedení diplomové práce, za cenné rady a připomínky během tvorby mé diplomové práce. Zároveň bych rád poděkoval svým kolegům z firmy Centr Group, speciálně oblastnímu řediteli pro Moravu této společnosti panu Radimovi Vlhovi za pochopení, poskytnutí informací a materiálů, ale i za čas strávený odbornými konzultacemi, bez kterých by tato práce nemohla vzniknout. V neposlední řadě bych chtěl poděkovat své rodině a přátelům za podporu při studiu, za vytvoření příjemného prostředí i veškerou další pomoc při zpracování diplomové práce.

Anotace

Diplomová práce se zabývá problematikou logistiky bezpečnostních procesů a technologií spojených s monitoringem chování zákazníků velkoobchodu. Jsou zde objasněny pojmy jako bezpečnost, zákazník, typologie pachatelů krádeží a bezpečnostní prvky monitorování v prostředí velkoobchodu. V analytické části práce je provedena analýza současného stavu technologií a procesů pro monitorování chování zákazníků. Na základě zhodnocení analýzy je zpracován návrh na zefektivnění bezpečnostních procesů a využití bezpečnostních technologií.

Klíčová slova

bezpečnostní procesy, bezpečnostní technologie, monitoring chování osob

Annotation

The diploma thesis deals with the issue of logistics security processes and technologies related to the monitoring of customer behaviour in wholesale trade. Concepts such as security, customer, typology of theft perpetrators and security elements of monitoring in a wholesale environment are explained. In the analytical part of the thesis, an analysis of the current state of technology and processes for customer behaviour monitoring is conducted. Based on the evaluation of the analysis, a proposal is made to improve the efficiency of security processes and the use of security technologies.

Keywords

security processes, security technologies, monitoring of people's behaviour

Obsah

Úvod.....	9
1 Teoretická východiska problematiky monitoringu chování zákazníků	11
1.1 Pojetí bezpečnosti	11
1.2 Definice zákazníka	12
1.3 Typologie pachatelů krádeží	13
1.3.1 Psychologické hledisko pachatele	13
1.3.2 Kriminologické hledisko pachatele	14
1.3.3 Empirické hledisko pachatele	15
1.4 Bezpečnostní monitorování v prostředí velkoobchodu	16
1.4.1 Hlídací a detektivní služby	16
1.4.2 Technická ochrana	19
1.4.3 Legislativní požadavky	26
1.5 Kodex chování	30
2 Monitoring osob ve specifickém prostředí obchodu	32
2.1 Vybraná velkoobchodní jednotka	32
2.1.1 Charakteristika společnosti	32
2.1.2 Velkoobchodní jednotka	32
2.2 Podezřelé chování a jeho monitoring	33
2.2.1 Cyklus před útokem	33
2.2.2 Detekce podezřelého chování	35
2.2.3 Znaky podezřelého chování	36
2.3 Analýza současného stavu technologií a procesů pro monitorování chování zákazníků	38
2.3.1 Bezpečnostní systémy a bezpečnostní technologie vybrané velkoobchodní jednotky	38
2.3.2 Systém Altworx	39
2.3.3 Ochrana lidských zdrojů a osobních údajů	39
2.3.4 Identifikace problémů spojených s monitoringem	40

3	Návrh zefektivnění bezpečnostních procesů a technologií monitoringu	42
3.1	Zhodnocení analýzy stávajícího kamerového systému	42
3.1.1	Analogový kamerový systém	43
3.1.2	Digitální kamerový systém.....	43
3.2	Zhodnocení analýzy stávající fyzické ostrahy	44
3.2.1	Úkony pracovníků soukromé bezpečnostní služby	44
3.3	Zhodnocení analýzy stávající ochrany za pomoci pevných bezpečnostních prvků	46
3.4	Návrh pro nastavení bezpečnostních procesů za účelem zefektivnění monitoringu....	47
3.4.1	Modernizace kamerového systému	47
3.4.2	Úprava režimu fyzické ostrahy	51
3.4.3	Navýšení pevných bezpečnostních prvků	53
3.5	Riziko selhání RFID systému	56
4	Vyhodnocení přínosů návrhu	59
4.1	Modernizace kamerového systému	59
4.1.1	Kompaktní IP kamery vnitřní	60
4.1.2	Kompaktní mini hybridní termokamera	60
4.1.3	Cenová kalkulace	60
4.2	Navýšení fyzické ostrahy	61
4.2.1	Pracovník ostrahy parkoviště	61
4.2.2	Detektiv prodejny	61
4.2.3	Cenová kalkulace	62
4.3	Navýšení pevných bezpečnostních prvků	62
	Závěr	63
	Seznam zdrojů.....	65
	Seznam grafických objektů.....	68
	Seznam zkratek	69
	Seznam příloh	70

Úvod

S pojmem logistika se lze historicky setkat po mnoho století. Nikdy dříve jí ale nebylo věnováno tolik pozornosti, které se jí nyní dostává. Logistické procesy se jak ve výrobě, tak se uplatňují také v prodejní činnosti obchodních jednotek. Obchodní jednotky jsou jedním z článků logistického řetězce. Zákazníkům umožňují nákup různých položek zboží.

Chování zákazníků z hlediska problematiky bezpečnostních procesů a technologií podléhá neustálým změnám. Do popředí se dostává stále více tlak ekonomiky, kdy dochází k nárůstu obyvatel ohrožených takzvanou příjmovou chudobou. V současné době je podle statistických údajů v přímém ohrožení zhruba 1 milion obyvatel České republiky. Zároveň nelze opomínat rozvoj technologií, dále rozvoj výpočetní techniky a také nelze opomenout i změny v hospodářském prostředí. V souvislosti s tím nastává sofistikace u potencionálních pachatelů krádeží v prostředí velkoobchodu. Jinými slovy je možné říct, že člověk mající pochybné úmysly byl, a zároveň vždy bude o krok napřed před provozovateli obchodu.

Tuzemské firmy mají zájem o ochranu svého zboží před nekalými praktikami zákazníků, na druhé straně se oproti tomu snaží maximálně snižovat náklady spojené s bezpečnostní politikou ve svých provozovnách. Do popředí se dostává trend převodu povinností fyzické ostrahy do podoby automatizace. Také koncepce logistiky už nezahrnuje pouze fyzické toky zásob, či zboží od dodavatele k zákazníkovi, skladovou logistiku, či distribuci. Naopak začíná stoupat její vliv v mnoha jiných odvětvích, mimo jiné spojených i s bezpečnostními procesy a technologiemi. Postupně se ukazuje, že logistika je buď slabým místem celého řetězce, nebo naopak pomáhá šetřit čas, náklady, či dává strategické zvýhodnění v podobě konkurenční výhody.

Cílem této diplomové práce je využít poznatky bezpečnostních procesů a technologií při analýze a profilaci podezřelého chování zákazníků velkoobchodu. Získané informace následně využít pro nastavení bezpečnostních procesů velkoobchodu za účelem zefektivnění monitoringu podezřelých osob.

Diplomová práce je rozdělena do čtyř kapitol. V první kapitole je teoretické východisko problematiky spojené s monitoringem zákazníků, které se týká specifického prostředí velkoobchodu z hlediska komerční bezpečnosti. V druhé kapitole je zpracována

problematika tématu práce, ve které je věnován prostor praktickému charakteru logistiky bezpečnostních procesů pro potřeby návrhu zefektivnění bezpečnostních procesů a technologií. Návrh na zlepšení bezpečnostních procesů a technologií je zpracován ve třetí kapitole. V poslední, čtvrté kapitole, je zhodnocen reálný přínos návrhu bezpečnostních opatření pro potřeby konkrétního velkoobchodu.

Všechny informace potřebné pro analýzu v praktické části diplomové práce jsou čerpány z interních materiálů společnosti provozující velkoobchod na území České republiky. Zároveň vycházím z poznatků získaných v průběhu své doposud získané praxe v oblasti komerční bezpečnosti.

1 Teoretická východiska problematiky monitoringu chování zákazníků

V podmínkách různých obchodních jednotek je nezbytné za účelem bezpečnosti monitorovat prostory a také chování zákazníků. Tato kapitola se zabývá teoretickými východisky k dané problematice.

1.1 Pojetí bezpečnosti

Každý z nás si představí něco jiného pod pojmem bezpečnost podle toho, jaký druh bezpečnosti má právě na mysli. Shodu lze nalézt v tom, že pojem bezpečnost představuje určitou míru jistoty, která v lidech snižuje pocit ohrožení.

S pojmem bezpečnosti se setkáváme již od počátku naší existence. Způsob využití bezpečnostních procesů, včetně důvodů jejich zavedení, se v průběhu historie měnily, avšak primárním cílem bezpečnosti byly vždy následující tři skupiny:

- bezpečnost a ochrana zdraví, resp. života,
- bezpečnost a ochrana majetku,
- bezpečnost a ochrana informací.

Všechny tři skupiny se vzájemně často prolínají. Pro řešení bezpečnostní problematiky se u konkrétních subjektů vyžaduje vždy posuzování individuální situace a zájmů, které vykazuje dotčený subjekt. Existují tři otázky, na které si musí každý subjekt vždy odpovědět:

- zda a co má být chráněno,
- jaké hrozbě čelí předmět ochrany,
- jakým způsobem a jakými prostředky lze předmět ochrany chránit.

Každá z odpovědí na tyto otázky je závislá na řadě okolností, které se z hlediska ochrany subjektu rozdělují na vnitřní a vnější. Jako vnější okolnosti lze označit zejména existenci hrozby a míru rizika, s jakou se konkrétní hrozba může uskutečnit. Mezi vnitřní okolnosti lze zařadit okolnosti vycházející např. z ekonomických možností subjektu, realizace nutných bezpečnostních opatření. [1]

1.2 Definice zákazníka

Každý člověk se v průběhu života dostal nespočetněkrát do role zákazníka. Za zákazníka či klienta lze považovat kohokoliv, kdo naváže kontakt s obchodníkem. U obchodníka nakupujeme různé druhy zboží nebo přijímáme službu. V prostředí velkoobchodu vstupuje zákazník do prodejny, prohlíží či porovnává nabízený sortiment obchodu, získává, popř. se doptává na informace týkající se zboží. Následně zákazník může (ale také nemusí) realizovat samotný nákup.

Je třeba rozlišovat pojmy zákazník a spotřebitel. Tyto pojmy se velmi často zaměňují, přestože každý z nich má zcela odlišný význam. Spotřebitel je člověk, který zakoupené zboží využívá (resp. spotřebovává). Není zde ale podmínka, že se spotřebitel musí samotného úkonu nákupu zúčastnit. Lze tedy říct, že zákazník může být jak samotným kupujícím, tak zároveň i spotřebitelem. Opačně už to platit nemusí. Spotřebitel nemusí být ani kupujícím, a také ani zákazníkem. Pro úplnost je potřeba dodat, že kupující nemusí nutně výrobky spotřebovávat.

Problematiku koupě upravuje v českém právu občanský zákoník. [2] Podle ustanovení § 2075 a následujících se „*kupní smlouvou prodávající zavazuje, že kupujícímu odevzdá věc, která je předmětem koupě, a umožní mu nabýt vlastnické právo k ní, a kupující se zavazuje, že věc převezme a zaplatí prodávajícímu kupní cenu.*“ [2, § 2075]

Prodávající stanoví kupní cenu i případné slevy z ceny. Zároveň prodávající kupujícímu spolu se zbožím odevzdá i doklady, které se ke zboží vztahují, a umožní kupujícímu nabýt vlastnického práva k zakoupenému zboží v souladu s kupní smlouvou. Převzetím koupené věci nabývá kupující k věci vlastnické právo. V případě, že se jedná o samoobslužný prodej, nabude kupující vlastnické právo k věci zaplacením kupní ceny. Do té doby může kupující vrátit věc na původní místo. Pokud by vznikla na věci škoda ještě před zaplacením kupní ceny, nahradí se podle obecných ustanovení. [2]

Kupní smlouva podle zákona nemusí být uzavřena v písemné formě. V prostředí obchodních jednotek se jedná o ústní uzavření kupní smlouvy, nebo častěji tzv. konkludentně (beze slov).

I když v podmínkách obchodních jednotek má docházet k prodeji zboží, kdy zákazník za koupené zboží zaplatí a převezme si ho, tak praxe ukazuje, že v různých případech za různých okolností tomu tak není a dochází ke krádežím.

1.3 Typologie pachatelů krádeží

Problematiku krádeže upravuje v českém národním právu trestní zákoník, a to v § 205. Krádeže se dopouští ten, kdo si přisvojí cizí věc tím, že se jí zmocní a:

- „způsobí tak na cizím majetku škodu nikoliv nepatrnou,
- čin spáchá vloupáním,
- bezprostředně po činu se pokusí uchovat si věc násilím nebo pohrůzkou bezprostředního násilí,
- čin spáchá na věci, kterou má jiný na sobě nebo při sobě, nebo
- čin spáchá na území, na němž je prováděna nebo byla provedena evakuace osob.“ [3, § 205]

Obecně je rozdělení pachatelů krádeží velmi obtížné, jelikož zahrnuje velkou a složitou škálu lidí. Podle Čírtkové [4] je možné rozdělit typy pachatelů do skupin podle tří hledisek:

- psychologické hledisko pachatele,
- kriminalistické hledisko pachatele,
- empirické hledisko pachatele.

1.3.1 Psychologické hledisko pachatele

Dle psychologického hlediska se rozlišují následující typy pachatelů: rebelové, reakcionáři, slaboši a podivíni.

- Rebelové – tito pachatelé mají velké problémy s uvědoměním si hodnotového žebříčku, resp. nemají schopnost rozlišovat a brát v potaz případné následky spojené s krádeží.
- Reakcionáři – skupina pachatelů, kterou lze charakterizovat jako osoby, které mají problém s naplněním osobních životních cílů a tak jdou proti proudu. Zároveň se snaží škodit ostatním.
- Slaboši – osoby, které mají problém v obou výše zmíněných oblastech. Na tyto osoby sedí charakteristika jak rebelů, tak reakcionářů.
- Podivíni – tuto skupinu lidí lze charakterizovat tak, že mají problém sami se sebou. Tito lidé nemají vnitřní vyrovnanost. [4]

1.3.2 Kriminologické hledisko pachatele

Rozdělení z kriminologického hlediska pachatele dle Čírtkové [4] je na pachatele příležitostné, cílevědomé, plánovité, strategické a na recidivisty. S osobností pachatele pracuje kriminologická psychologie. Zabývá se zdrojem kriminality, dále sociálními a psychologickými podněty.

- Příležitostní pachatelé krádeží – si svou trestnou činnost předem neplánují a do obchodu nepřichází s úmyslem krást. Prvotním a spouštěcím signálem je až fakt, že zboží není v danou chvíli dostatečně, resp. vůbec zabezpečeno proti krádeži. Typickým příkladem je sortiment alkoholických nápojů, kde nejsou lahve zvlášť zabezpečeny ochranným prvkem. Velmi dobře lze využít přísloví, že příležitost dělá zloděje. Naopak pokud vidí pachatel kvalitní zabezpečení zboží, popř. jiná fungující bezpečnostní opatření, zpravidla svého chování zanechá a svůj úmysl si rozmyslí.
- Cílevědomí pachatelé – jsou přesným opakem příležitostných pachatelů. Tato skupina osob již vstupuje do prostoru prodejny s úmyslem krást a v případě potřeby za tímto účelem i překonávat bezpečnostní opatření. Zároveň jsou tyto osoby předem seznámeny s možnými riziky a následky jejich chování a činů.
- Plánoví pachatelé – pro svůj úmysl krádeže absolvují mnohem delší a kvalitnější přípravu než cílevědomí pachatelé. Tyto osoby mají skvělý přehled o bezpečnostních opatřeních prodejny a v případě komplikací mají často připravený záložní plán. Při svém plánování překonávání bezpečnostních opatření si předem zjišťují možnosti jejího překonání. Pro tyto účely jsou také často vybaveny různými prostředky pro snadnější průběh celé krádeže.
- Strategičtí pachatelé – jsou to osoby, které se krádeží často ani přímo neúčastní. Na místo toho posílají za sebe krást jiné osoby, popř. skupiny osob. Často se jedná o osoby mladistvé, na které se nevztahuje trestní odpovědnost za způsobené škody. Z praxe se může jednat o dospělou osobu, která ke krádeži nabádá své vlastní děti.
- Recidivisté – jsou to lidé, pro které se krádeže stávají životním stylem. S krádežemi mají z minulosti velké zkušenosti, ke krádežím dochází opakovaně. Tyto osoby nemají v plánu se krádežím vyvarovat do budoucna, a to ani v případě hrozby odsouzení a následného pobytu ve vězení. Už jen představa o jiné životní dráze je pro ně nepředstavitelná.

1.3.3 Empirické hledisko pachatele

Z empirického hlediska rozděluje Čírtková [4] pachatele na vývojové, příležitostné, recidivující, pachatele v ekonomické tísní a psychicky nemocné pachatele.

- Vývojoví pachatelé – jedná se buď o skupinu nezletilých dětí a mladistvých do věku 21 let, nebo o skupinu osob starších šedesáti let. Pozadím pro motivaci páchaní krádeží je v tomto případě vývojový faktor. V případě nezletilých, resp. mladistvých pachatelů se často uplatňuje jejich celková emocionální nestabilita a nevyzrálost. Motivem krádeže se stává touha po dobrodružství, snaha po uznání u svých vrstevníků, pokus o seberealizaci či blíže nespecifikovaný druh protestu. V případě osob starších šedesáti let se lze setkat s pokusy o krádež spíše výjimečně. Pokud kradou, jedná se často o osoby, které mají nějaké duševní onemocnění, kdy si tato osoba vlastně ani neuvědomuje, že se pokusila o krádež, nebo že kradla.
- Příležitostní pachatelé – tato skupina osob zahrnuje naprostou většinu pachatelů krádeží. V podstatě se jedná o běžnou osobu, kterou na první pohled nelze rozlišit od ostatních. Jediným rozlišovacím znakem je pouze fakt, že se dopustili krádeže zboží v prodejně. Ani následným dotazováním není pachatel schopen vysvětlit svou motivaci krádeže. Nemá žádnou duševní poruchu osobnosti, nekoná ani z pomsty či pro finanční tíseň. Pouze uskutečnil nápad, který ho v danou chvíli napadl. A zároveň vnímal celou situaci jako situaci bez rizika. Tato osoba je si vědoma svého činu, pouze není schopna své jednání adekvátně vysvětlit. Určitou roli v těchto situacích může hrát emoční vypětí, frustrace či neukojený pocit spokojenosti.
- Recidivující pachatelé – takovouto osobu pachatele lze označit již za chronického zloděje, či dokonce za profesionálního zloděje. Tyto osoby se pohybují na úplném okraji společnosti a představa návratu do normálního života je pro ně nepředstavitelná, resp. frustrující. Důvodem pro krádeže jsou otázky existenčního hlediska a potřeb. Z hlediska veřejnosti představují nejvýraznější skupinu pachatelů, ale ne nejpočetnější. Hrozba vězení či jiného trestního postihu pro ně nemá dostatečný odstrašující účinek, který by je odradil od dalších krádeží.
- Pachatelé v ekonomické tísní – pachatel se dopouští odcizení zboží z důvodu, že jej nutně potřebuje, popř. je přesvědčen o tom, že jej nutně

potřebuje. K nákupu takového zboží ale nemá dostatek finančních prostředků a tak zboží raději odcizí.

- Psychicky nemocní pachatelé – nepochybně se jedná o nejspornější, a zároveň o nejdiskutovanější skupinu pachatelů s ohledem na možnou diskuzi hranic duševního zdraví. Typickým příkladem je nemoc zvaná kleptomanie. Nejedná se ve své podstatě o zpochybnění jasně definovaných psychiatrických diagnóz. [4]

1.4 Bezpečnostní monitorování v prostředí velkoobchodu

K zajištění bezpečnosti obchodní jednotky, ochrany majetku a osob, je nezbytné provádět bezpečnostní monitorování. Za tímto účelem lze využít:

- **hlídací a detektivní služby,**
- **technickou ochranu.**

Použití těchto prvků musí být vždy v souladu s legislativními požadavky.

1.4.1 Hlídací a detektivní služby

Bezpečnostní monitorování, nebo také bezpečnostní sledování, či pozorování je nedílnou součástí pro bezpečnost a ochranu majetku v prostředí velkoobchodu. Jedná se o sloučení fyzické i technické ochrany. Ty jsou navzájem spojeny tak, aby byla maximalizována snaha k zamezení škod, příp. alespoň k jejich minimalizaci. Jmenovitě se jedná o sběr a následné zpracování informací, činnost dohledového centra a vyhodnocení informací v čase jak reálném, tak pozdějším z důvodu činnosti dohledávání v prostorech velkoobchodu.

Podle Lukáše [5, s. 166] patří fyzická ostraha: „*mezi základní pilíře v poskytování ochrany majetku a osob. Ve většině případů bývá doplněna technickými prostředky, ale ať je technologie sebelepší, nemůže plně nahradit lidský faktor. Vždy bude potřeba, aby pracovník průmyslu komerční bezpečnosti (dále jen PKB) vyhodnotil danou situaci a adekvátně na ni zareagoval.*“

Zaměstnanci soukromé bezpečnostní služby při výkonu povolání využívají všech dostupných prostředků – kamerové systémy, elektronická zabezpečovací zařízení,

podporu dohledového přijímacího poplachového centra a příp. služeb detektiva, pokud jím velkoobchodní jednotka disponuje.

„Fyzická ostraha zaujímá významné místo v ochraně majetku a osob. Její důležitost přetrvává i s rozmachem technických prostředků, které se do bezpečnosti zapojují v posledních letech čím dál tím více. Fyzická ostraha je neoddiskutovatelnou součástí komplexního zabezpečení majetku a osob. Nutnost pracovníka průmyslu komerční bezpečnosti (dále jen PKB) je zejména v těch situacích, kdy je potřeba rychlý zákrok proti protiprávnímu jednání, rychlá reakce nebo obecně rozhodovací proces. Pracovník může řadu nechtěných situací vyřešit preventivně, nebo jim zabránit hned v počátcích. Proto je důležitý nejen výběr těchto osob, ale také jejich výcvik, aby dokázali včas rozpoznat mimořádnou událost, konfliktní situaci nebo jakoukoli krizi, aby ji dokázali správně vyhodnotit a adekvátně zareagovat. Pracovníci PKB jsou téměř vždy na očích veřejnosti, proto je nezbytné, aby věděli, jak se mají zachovat, a tím šli nejen příkladem pro ostatní lidi, ale také aby přispěli k dobrému jménu své firmy a obecně tomuto oboru. Bohužel média jsou plná zpráv o situacích, kdy pracovník neví, jak jednat, nebo nerozpoznal nebezpečnou situaci. Potom klesá vážnost průmyslu komerční bezpečnosti a zejména jeho důvěryhodnost.“ [5, s. 164]

Hlídací a detektivní služby zahrnují činnost soukromých bezpečnostních služeb prostřednictvím soukromých bezpečnostních pracovníků a detektivů. Jedná se o fyzickou ostrahu a ochranu pro potřebu velkoobchodní jednotky. V širším pojetí sem lze zahrnout i činnost na ochranu předmětů, kontrolu vozidel, dohled při doprovodu cenností a finančních prostředků, příp. jejich samotný doprovod. Dále zahrnuje v konkrétním prostředí ochranu práv a svobod, příp. dalších zájmů dle konkrétních potřeb a požadavků.

V České republice doposud chybí zákon o soukromých bezpečnostních službách (SBS), přestože je tato činnost, resp. pravomoc poměrně přesně definována zákony. Pro efektivní výsledek práce je třeba ji přesně plánovat v podobě logistických kroků spojených s nastavením bezpečnostních procesů vhodných do prostředí velkoobchodu. Fyzická ostraha je hojně využívána také proto, že lze díky jejímu prostřednictví efektivně reagovat na nově vzniklé situace a v případě nutnosti provést bezprostředně bezpečnostní zásah. Tím dojde k zamezení přímo hrozícímu nebezpečí, příp. k minimalizaci škod.

Fyzická ostraha plní ve velkoobchodech zejména následující činnosti:

- Kontrola a dohled zejména při dodržování veřejného pořádku a norem občanského soužití, příp. dodržování dobrých mravů a v případě jejich narušení se provedou opatření k jejich následnému zamezení.
- Monitorování aktuální situace v prostředí velkoobchodu, obzvláště zabránění krádežím zboží či jiného majetku společnosti.
- V případě zjištění páchaní trestné činnosti dojde k zajištění zboží, pachatele, příp. důkazů, či svědků pro potřeby orgánů trestního řízení. Dále je zajištěno místo činu. Následně se okamžitě informují příslušné orgány (PČR, MP) a v případě zadržení pachatele dojde k jeho předání příslušným orgánům. O takové události je následně sepsán záznam, či jiné oznámení o mimořádné události. V poslední řadě je potřeba informovat odpovědnou osobu (osoby).
- Kontrola vstupu do zázemí prodejny nepovolaným osobám, příp. vyvedení těchto osob.
- **Typování** a monitorování zlodějů (např. kapesních). Svou přítomností jsou součástí preventivních opatření.
- Obsluha elektronických zařízení – zabezpečovacích a protipožárních (EZS, EPS).
- Kamerový dohled při přepravě finančních prostředků, popř. fyzický doprovod.
- Kontrolní činnost v prostorech pokladní zóny, kde sleduje nejen zákazníky, ale provádí kontrolní činnost také nad zaměstnanci velkoobchodu.
- Plnění a zajištění protipožární ochrany prostoru velkoobchodu, příp. dodržování hygienických opatření (např. v době pandemie Covid-19 dodržování protipandemických opatření).
- Dodržování pokynů klienta (objednatele) – dohled nad zaměstnanci velkoobchodní jednotky, zakázaný prodej podomního prodeje, žebrání u zákazníků či dodržování pracovní doby zaměstnanců.
- Vedení klíčového režimu, včetně odemykání a zamykání prodejny v době provozní doby. Dále odemykání/zamykání dalších prostor uvnitř jednotky.
- Doplňková činnost pro potřeby velkoobchodu – kontrola služebního vchodu, vjezd a výjezd do areálu prodejny pro dodavatele, informování zákazníků.
- Další povinnosti vycházející z platné smlouvy mezi klientem (objednavatelem) a zprostředkovatelem (SBS).



Obr. 1.1 Pracovník SBS v prostoru velkoobchodu

Zdroj: vlastní zpracování.

1.4.2 Technická ochrana

Technická ochrana je systémem ochrany, která používá technické bezpečnostní prostředky, které slouží k tomu, aby zabránily, ztížily, nebo oznámily narušení chráněného prostoru. Například kamerové systémy, poplachové zabezpečovací systémy a jiné. Prostředky technické ochrany lze použít pro zajištění odstrašení pachatele. Přestože pachateli v ničem nebrání, jsou ve spolupráci s fyzickou ostrahou pokládány za velmi spolehlivý způsob ochrany [6]

V publikaci *Bezpečnostní technologie, systémy a management* autor Lukáš uvádí, že „v dnešní době nastává trend, že hodně odborníků i klientů odstupuje od fyzické ostrahy a její místo je nahrazováno systémy technické ochrany (poplachové zabezpečovací a tísňové systémy, kamerové systémy atd.). Nastává potom situace, že objekt je sice skvěle technicky zabezpečen, ale již není přítomen nikdo, kdo by na poplach reagoval, nebo spíše je vzdálen tak daleko, že není možný okamžitý zásah proti narušiteli. Nezbytné je, aby tyto dvě oblasti spolu spolupracovaly. Jakoukoli technikou nelze

nahradit lidský faktor. Jeho intuici, předvídatost, rychlost rozhodování a zejména možnost reakce.“ [5, s. 164]

Kombinací fyzické a technické ochrany lze docílit vyšší a efektivnější ochrany objektu. V případě velkoobchodní jednotky je potřeba zmínit zejména elektronickou ochranu zboží bezpečnostními prvky i kamerové systémy. Technickou ochranou se rozumí i systémy elektronického zabezpečení, které slouží k zabránění nedovoleného vniknutí do vnitřních prostor objektu, systémy, které předávají informace pracovníkům SBS o případném narušení objektu, a zároveň slouží ke ztížení přístupu pachatelů.

1.4.2.1 Elektronické zabezpečení zboží

K eliminaci krádeží využívají velkoobchody tzv. EAS systémy (electronic article surveillance). Volně lze tento systém přeložit jako elektronické sledování předmětů.

Pokud je zboží řádně zapláceno, jsou bezpečnostní prvky odstraněny či deaktivovány.

„Elektromechanické detektory patří z historického hlediska k nejstarším detekčním prvkům využívaným v systémech technické ochrany. I přes svou historickou pozici si však svou nezastupitelnou roli našly i v současných sofistikovaných formách technické ochrany. Své uplatnění nachází v dnešní době v ochraně obvodové, plášťové, prostorové i předmětové“. [7, s. 38]

Hlavním prvkem těchto systémů jsou antény. Ty pracují na bázi technologie radiofrekvenční identifikace. Jedná se o elektronickou ochranu zboží za pomoci RFID, což je radiofrekvenční identifikace zboží. Je to technologie, při které jsou digitální data zapsaná v RFID tagu, nebo tzv. chytré etikety, jsou přečtena snímačem za použití radiového elektromagnetického vlnění. K zachycení dat z tagu se používají radiové vlny. RFID nevyžaduje pro přečtení uložených dat přímou viditelnost, zapsaná data lze snadno měnit, systém má vysokou spolehlivost a velmi rychlé čtení přinášející výraznou úsporu času.

Nespornou výhodou těchto systémů jsou relativně nízké pořizovací náklady stejně jako následné náklady na provoz.

Při zohlednění počtu krádeží, resp. výše příp. škod je tento systém vhodnou implementací. Pro zajištění správné funkčnosti EAS systému (elektronické sledování

předmětů) musí být ve velkoobchodě instalovány detekční brány, programové vybavení systému, vhodně zvolené a použité RFID tagy, deaktivátory RFID tagů a RFID čtečky.



Obr. 1.2 Ochranný rám

Zdroj: [8].

Systém se skládá z následujících komponentů:

- pevné prvky zabezpečení zboží (plastové a jiné speciální ochranné etikety, samolepky),
- deaktivátor ochranných etiket, příp. uvolňovač pevných prvků,
- detekční brány pro účely vytvoření a zabezpečení ochranného prostoru.

Příslušenství EAS systémů:

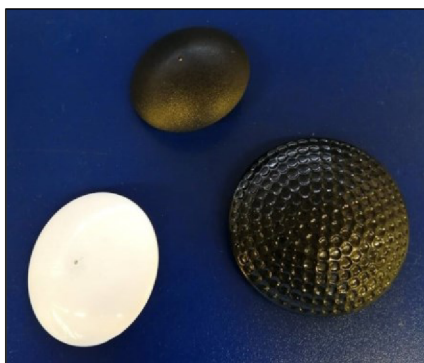
Samolepící etikety – často jsou potisknuty falešnými čárovými kódy tak, aby pachatel krádeže nedokázal tento prvek rozpoznat. Jejich velikost je různá, využívají se na nekovové zboží a lze je bezdotykově deaktivovat. Příklad tzv. měkké etikety je na obrázku 1.3.



Obr. 1.3 Měkká etiketa

Zdroj: [9].

Tvrde etikety – se zbožím jsou spojeny buď bezpečnostním lankem, nebo kovovým pinem. Často jsou využívány pro zabezpečení dražšího textilního zboží, či dražších domácích potřeb a elektronického zboží. Jejich odjištění se provádí za pomoci speciálního uvolňovače na bázi magnetu. Příklad tzv. tvrdé etikety je na obrázku 1.4.



Obr. 1.4 Tvrdá etiketa

Zdroj: vlastní zpracování.

Plastová etiketa – je stahovací etiketa určená převážně k ochraně lahví. Uvnitř plastové etikety je vloženo ocelové lanko – viz příklad na obrázku 1.5.



Obr. 1.5 Plastová etiketa chránící lahev alkoholu před krádeží

Zdroj: vlastní zpracování.

Bezpečnostní obaly – se využívají k zabezpečení drobné elektroniky, drogerie, či dražších menších potravin. V obalu je zabudována bezpečnostní cívka, často lze obal zavěsit do regálu.

Příklad bezpečnostního obalu je na obrázku 1.6.



Obr. 1.6 Bezpečnostní obal

Zdroj: vlastní zpracování.

Jehly a lanka – oba bezpečnostní prvky jsou příslušenstvím pro upevnění etiket na zboží. Zboží je zajištěno lankem či jehlou, které se zacvakne do etikety. V případě poškození zvukových jehel dojde k aktivaci zvukového tónu, který dosahuje hlasitosti vyšší než 100 dB. Příklad těchto bezpečnostních prvků je na obrázku 1.7.



Obr. 1.7 Bezpečnostní prvek s integrovaným lankem

Zdroj: [10].

Speciální etikety – bezpečnostní prvky vytvořené přímo pro daný sortiment. V praxi se lze setkat se speciální bezpečnostní etiketou na brýle, příp. na zabezpečení drahého alkoholu.



Obr. 1.8 Speciální bezpečnostní etiketa

Zdroj: [11].

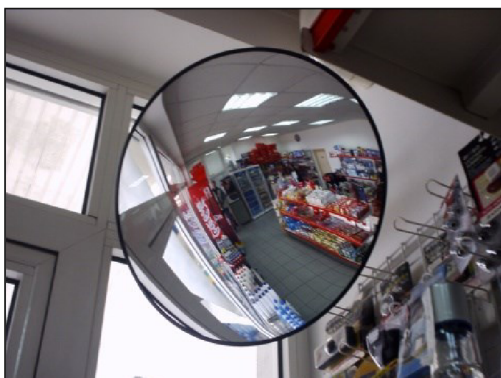
Smyčková ochrana – se používá pro zboží, které se má zabezpečit a to tak, že zbožím je protažen kabel tak, aby vytvořil ochrannou smyčku. V případě, že dojde k přerušení smyčky, je vyvolán poplach. Příklad zabezpečení je na obrázku 1.9.



Obr. 1.9 Smyčková ochrana

Zdroj: vlastní zpracování.

Bezpečnostní zrcadla – slouží jako doplněk při ochraně zboží. Jedná se o pasivní prvek bezpečnostní ochrany. Příklad viz obrázek 1.10.



Obr. 1.10 Bezpečnostní zrcadlo

Zdroj: [12].

Deaktivace

Deaktivátory pevných bezpečnostních prvků – se používají v případě zabezpečení zboží pomocí RFID tagů. Princip použití je takový, že přiložením tagů na plochu deaktivátoru se zboží deaktivuje. Pokud tak není učiněno, RFID tag bude nadále aktivní a dojde ke spuštění EAS systému, resp. ke spuštění poplachu při průchodu detekční bránou.

Pro deaktivaci pevných etiket se využívá tzv. uvolňovač. Uvnitř je umístěn silný magnet, který přiložením pevné etikety uvolní ochranný prvek.



Obr. 1.11 Uvolňovač etiket

Zdroj: [13].

1.4.2.2 Kamerové systémy

Kamerové systémy jsou nepochybně významným prvkem pro rozšíření ochrany zboží. Za pomoci kamerového systému může pracovník bezpečnostní služby lokalizovat případného pachatele, provést rychlý zásah při dopadení pachatele, příp. za pomoci tohoto systému zdokumentovat jednání pachatele jako důkazní materiál.

Celý systém je vhodné používat nejen v prodejních prostorech velkoobchodu (prodejní plocha, pokladní zóna atd.), ale i v zázemí velkoobchodu, kde se pohybují zaměstnanci či dodavatelé (skladové prostory, kanceláře, služební vchod a jiné).

Zároveň lze využít kamerový systém i pro další kontrolní činnost velkoobchodu. Příkladem je implementace kamerových systémů do pokladní zóny, kde pracovníci SBS mohou kontrolovat správnost markování zboží, krádeže zaměstnanců peněžních prostředků či využít kamerový systém v případě reklamace zákazníka.

Kamerový systém lze instalovat dvěma způsoby – viditelně, nebo skrytě. Vhodnou volbou je kombinace kamerového systému s prvky EZS či EAS systémů.

Základní rozdělení kamerových systémů:

Analogové kamerové systémy – princip používání analogových kamerových záznamů je založen na přenosu signálu z kamery v analogové podobě. K přenosu signálu z kamery je nejčastěji využíván běžný koaxiální kabel. Omezením tohoto řešení je závislost kvality přenášeného signálu na základě délky vedení koaxiálního kabelu. Maximální doporučená délka je přibližně 100 m.

Výhodou využívání analogových kamerových systémů je jejich jednoduchá obsluha, včetně nenáročné instalace bezpečnostních kamer. Náklady na pořízení analogového systému jsou nižší ve srovnání s IP kamerovým systémem. Dalším kladem při využívání tohoto systému je kompatibilita bezpečnostních kamer od jiných výrobců.

Nevýhodou systémů je rozlišení analogových kamer, které je limitováno daným formátem. Analogová technologie není schopna provádět přenos celého obrazu najednou. V porovnání s IP kamerovým systémem je třeba vyšší počet kamer na ostrahu stejného prostoru.

IP kamerové systémy – v případě volby digitálního kamerového systému není v podstatě žádné omezení na maximální rozlišení přenášeného obrazu. To je limitováno pouze zvolenou kamerou, typem záznamového zařízení, příp. propustností datové sítě. Digitální kamerové systémy využívají pro přenos datový kabel, který zároveň uživateli umožňuje napájení kamer.

Největší výhodou využití digitálního kamerového systému v porovnání se zastaralým analogovým kamerovým systémem je bezpochyby jeho možnost vysokého rozlišení digitálního obrazu. Ten není omezen jako v případě analogového signálu. Přenos záznamů nabízí možnost sledování obrazu odkudkoliv. IP kamery jsou stále více v oblasti komerční bezpečnosti využívány pro účely umělé inteligence, i k propojení s dalšími bezpečnostními systémy.

Nevýhodou IP kamerového systému je vyšší pořizovací cena. Záznamy potřebují vyšší kapacitu na pevném disku rekordéru.

1.4.3 Legislativní požadavky

Pro bezpečnostní monitorování jsou v právních předpisech stanovena pravidla pro použití bezpečnostních prvků. Použití musí být vždy v souladu s těmito legislativními požadavky.

Legislativní požadavky lze rozdělit podle právních předpisů na předpisy týkající se:

- fyzické ostrahy,
- technické ochrany.

Právní úprava fyzické ostrahy

Z hlediska fyzické ostrahy velkoobchodní jednotky je třeba brát v potaz, že do dnešního dne je stále absence zákona, který by upravoval činnost služeb soukromých bezpečnostních služeb. Soukromé bezpečnostní služby se však při výkonu své služby mohou opřít o zákon č. 40/2009 Sb., trestní zákoník. Konkrétně o hlavu III – okolnosti vylučující protiprávnost činu. Dále také o znění příslušných paragrafů trestního řádu, tj. zákona č. 141/1961 Sb., o trestním řízení soudním.

- **Krajní nouze – § 28 trestního zákoníku:** *„Čin jinak trestný, kterým někdo odvrací nebezpečí přímo hrozící zájmu chráněnému trestním zákonem, není trestným činem. Nejde o krajní nouzi, jestliže bylo možno toto nebezpečí za daných okolností odvrátit jinak anebo způsobený následek je zřejmě stejně závažný nebo ještě závažnější než ten, který hrozil, anebo byl ten, komu nebezpečí hrozilo, povinen je snášet.“* [3, § 28]

Podstatou krajní nouze je odvrácení přímo hrozícího nebezpečí zájmům chráněných trestním zákonem, příp. zmírnění již neodvratitelných následků, které by za jiných okolností byly samy trestným činem. Podmínkou pro splnění těchto požadavků je odvrácení nebezpečí, které nesmí být v konečném důsledku stejné nebo ještě vyšší. Typickým příkladem je v případě požáru v prostorech velkoobchodu rozbití výlohy tak, aby zákazníci mohli bezpečně prostory prodejny opustit. Za normálních okolností by rozbití výlohy bylo trestným činem, ale v celém kontextu situace je to správné využití krajní nouze.

- **Nutná obrana – § 29 trestního zákoníku:** *„Čin jinak trestný, kterým někdo odvrací přímo hrozící nebo trvajících útok na zájem chráněný trestním zákonem, není trestným činem. Nejde o nutnou obranu, byla-li obrana zcela zjevně nepřiměřená způsobu útoku.“* [3, § 29]

Podstatou nutné obrany je odvrácení útoku na zájem chráněný trestním zákonem. Podobně jako u krajní nouze by se osoby za normálních okolností dopouštěly odvrácením útoku protiprávního jednání. Protože ale osoba, která útok odvrací, chrání zájmy trestního zákona, nedopouští se sama trestného činu. Při využití nutné obrany musí být odvrácení efektivní, a proto může osoba odvracející útok využít přiměřeně vyšší síly právě z důvodu rychlého a efektivního odvrácení útoku. Je třeba podotknout, že obrana nesmí být zcela

zjevně nepřiměřená míře útoku. Zároveň nesmí obrana pokračovat v době, kdy již útok skončil.

- **Svolení poškozeného – § 30 trestního zákoníku:** „*Trestný čin nespáchá ten, kdo jedná na základě svolení osoby, jejíž zájmy, o nichž tato osoba může bez omezení oprávněně rozhodovat, jsou činem dotčeny. Svolení podle odstavce 4 musí být dáno předem nebo současně s jednáním osoby páchající čin jinak trestný, dobrovolně, určitě, vážně a srozumitelně; je-li takové svolení dáno až po spáchání činu, je pachatel beztrestný, mohl-li důvodně předpokládat, že osoba uvedená v odstavci 1 by tento souhlas jinak udělila vzhledem k okolnostem případu a svým poměrům. S výjimkou případů svolení k lékařským zákrokům, které jsou v době činu v souladu s právním řádem a poznatky lékařské vědy a praxe, nelze za svolení podle odstavce 1 považovat souhlas k ublížení na zdraví nebo usmrcení.*“ [3, § 30]
- **Přípustné riziko – § 31 trestního zákoníku:** „*Trestný čin nespáchá ten, kdo v souladu s dosaženým stavem poznání a informacemi, které měl v době svého rozhodování o dalším postupu, vykonává v rámci svého zaměstnání, povolání, postavení nebo funkce společensky prospěšnou činnost, kterou ohrozí nebo poruší zájem chráněný trestním zákonem, nelze-li společensky prospěšného výsledku dosáhnout jinak. Nejde o přípustné riziko, jestliže taková činnost ohrozí život nebo zdraví člověka, aniž by jím byl dán k ní v souladu s jiným právním předpisem souhlas, nebo výsledek, k němuž směřuje, zcela zřejmě neodpovídá míře rizika, anebo provádění této činnosti zřejmě odporuje požadavkům jiného právního předpisu, veřejnému zájmu, zásadám lidskosti nebo se přiči dobrým mravům*“. [3, § 31]
- **Oprávnění použití zbraně – § 32 trestního zákoníku:** „*Trestný čin nespáchá ten, kdo použije zbraně v mezích stanovených jiným právním předpisem*“. [3, § 32]
- **Zadržení osoby podezřelé – § 76 trestního řádu č. 141/1961 Sb.:** „*Osobní svobodu osoby, která byla přistižena při trestném činu nebo bezprostředně poté, smí omezit kdokoliv, pokud je to nutné ke zjištění její totožnosti, k zamezení útěku nebo k zajištění důkazů. Je však povinen tuto osobu předat ihned policejnímu orgánu; příslušníka ozbrojených sil může též předat nejbližšímu útvaru ozbrojených sil nebo správci posádky. Nelze-li takovou osobu ihned předat, je*

třeba některému z uvedených orgánů omezení osobní svobody bez odkladu oznámit.“ [14, § 76]

Jak vyplývá z výše uvedeného § 76, tak může být na osobní svobodě omezena kýmkoliv osoba přistižena při páchání trestného činu, nebo bezprostředně po spáchání trestného činu. Pro účely velkoobchodu se nejčastěji jedná o zadržení pachatele krádeže. Omezení osobní svobody je podmíněno dobou nezbytně nutnou, tedy do předání policejním orgánům, resp. příslušníkům ozbrojených sil. Pokud by nebylo takto učiněno, dopouští se osoba trestného činu omezení osobní svobody dle zákona č. 40/2009 Sb., trestního zákoníku.

Právní úprava technické ochrany

K preventivnímu zajištění bezpečnosti osob a majetku nacházejících se uvnitř velkoobchodní jednotky slouží uzavřený kamerový televizní systém (Closed Circuit TeleVision – CCTV). Pro účely preventivní bezpečnosti lze provozovat CCTV bez souhlasu vstupujících osob, neboť velkoobchodní jednotka na základě pořízených kamerových záznamů nezpracovává osobní údaje. Nejčastějším důvodem pro potřeby pořizování záznamů z kamerových systémů je jejich následné využití za účelem identifikace osob, které se dopustily protiprávního jednání.

I když 25. května 2018 vstoupil v platnost nový zákon na ochranu osobních údajů (GDPR), který mimo jiné upravuje původní systém pro zpracování pořízených kamerových záznamů a jejich následné uchování, na možnosti využití kamerových televizních systémů podle předchozího odstavce to nemá vliv.

Dle velikosti paměti serveru jsou pořízené záznamy uloženy pro případné dohledávání v rozsahu od 24 hod. až po dobu několika měsíců.

Z hlediska právní úpravy užití kamerových systémů je nutné rozlišovat, zda se jedná o kamerové systémy se záznamem, nebo o kamerové systémy bez záznamu.

Kamerové systémy se záznamem

Kamerové systémy se záznamem, jak už bylo zmíněno výše, v případě pořizování kamerových záznamů se jedná o zacházení s osobními údaji. Z tohoto důvodu je třeba kamerový systém zaregistrovat na Úřadě na ochranu osobních údajů. Výjimkou

z povinnosti registrovat kamerové systémy je situace, kdy je kamerovým záznamem chráněn majetek společnosti. V tomto případě se doporučuje vyvěsit upozornění na tento fakt, popř. upozornit formou výstražné tabule, či nálepky na střežení kamerovým systémem.

V případě registrace je třeba stanovit účel kamerového systému. Nejčastěji uváděným důvodem je ochrana osob a majetku. Dalšími podmínkami je zabezpečení systému před zneužitím, uchování záznamu na dobu nezbytně nutnou (poté smazání záznamů). Umístění kamery nesmí být na místě určeném k soukromým záležitostem (např. WC, sprcha, apod.).

Příklad informační tabule je na obrázku 1.12.



Obr. 1.12 Informační tabule o využití kamerového systému

Zdroj: [15].

Kamerové systémy bez záznamu

V případě kamerových systémů bez záznamu se musíme řídit pouze obecnými předpisy upravujícími ochranu osobnosti. O faktu, že je prostor snímán kamerovým systémem je třeba informovat (informační tabule/nálepka). Nelze umístit kamerový systém do prostoru, kde jsou vykonávány soukromé záležitosti (např. WC, sprcha, apod.).

1.5 Kodex chování

V souvislosti s Obecným nařízením EU o ochraně osobních údajů (GDPR) byl v ČR zřízen Úřad pro ochranu osobních údajů. Úřad mimo jiné s cílem vysvětlit podstatu kodexů chování v této oblasti uveřejnil příručku Kodexy chování. Příručka má pomoci veřejnosti, aby se lépe orientovala v této oblasti, přiblížila jí základní pravidla,

a zároveň doporučila praktické postupy v aplikaci pravidel chování. Kodex chování tedy stanovuje základní prvky zásad, postupy a požadavky na zpracování osobních údajů v konkrétních odvětvích. To se týká také zpracování a nakládání s osobními údaji v rámci obchodních jednotek. [16]

Kodex chování je dobrovolným systémem samoregulace. Musí být zpracován tak, aby pokryl požadavky upravené obecným nařízením o ochraně osobních údajů, a zároveň řešil specifika, která vznikají při zpracování osobních údajů v rámci daného odvětví (zde obchodu a velkoobchodu)

Příslušný subjekt může prokázat soulad s nařízením EU 2016/679 v oblasti GDPR zpracováním a dodržováním kodexu chování. Soulad s nařízením a dodržováním kodexu chování může kontrolovat tzv. dozorový orgán, kterým je v České republice Úřad pro ochranu osobních údajů. [16]

2 Monitoring osob ve specifickém prostředí obchodu

Obsahem této kapitoly jsou základní informace o konkrétní velkoobchodní jednotce. Zároveň je zde zpracována analýza současného stavu monitoringu osob v této vybrané velkoobchodní jednotce.

2.1 Vybraná velkoobchodní jednotka

Problematika tématu diplomové práce týkající se monitoringu osob v obchodu a uplatnění bezpečnostních procesů a technologií je řešena ve vybraném velkoobchodu Makro cash & carry ČR.

2.1.1 Charakteristika společnosti

Makro cash & carry ČR bylo založeno jako dceřiná společnost firmy SHV Makro. K 1. lednu 1998 převzala veškeré velkoobchodní aktivity společnosti SHV Makro v Evropě firma METRO AG.

Společnost Makro je obchodní řetězec, jenž provozuje samoobslužné obchodní domy fungující na systému cash & carry (zaplacení zboží a jeho následném odvezení). Zákazníky tvoří zejména klienti z oblasti gastronomie, obchodu, či prostředí hotelových služeb. V rámci celého světa má společnost METRO AG své pobočky ve 29 zemích. [17]

Na území České republiky provozuje společnost 13 prodejen. K nákupu ve společnosti Makro je třeba být držitelem tzv. Makro karty, kterou lze získat registrací. Registrace se provádí na základě předložení živnostenského listu, popř. na základě výpisu z obchodního rejstříku. Společnost Makro nabízí široký sortiment jak potravinářského, tak nepotravinářského zboží formou velkoobchodního prodeje registrovaným podnikatelům, obchodníkům a velkoodběratelům, jakými jsou nemocnice, školy, orgány státní správy apod.

2.1.2 Velkoobchodní jednotka

Pro praktickou část této diplomové práce je vybrána jedna z prodejen společnosti Makro. Tato prodejna spadá svou rozlohou zhruba 9 000 m² mezi menší prodejny na území ČR. Součástí velkoobchodní jednotky jsou také vyhrazená parkovací místa.

Ve svém sortimentu tato velkoobchodní jednotka nabízí více než 45 000 položek pro potřeby zákazníků. Prodejna Makro je otevřena pro zákazníky denně, a to v čase od 8 do 21 hodin. Zároveň umožňuje vybraným partnerům nákup zboží v pracovní dny již od 5 hodin ráno, v případě soboty od 6. hodiny ranní.

Konkrétní informace, které jsou zahrnuty v této práci, jsou získány na základě konzultací s vrcholovým managementem velkoobchodní jednotky. Dále jsou zde využity poznatky a praktické zkušenosti z vlastního pracovního zařazení autora diplomové práce na pozici bezpečnostního manažera soukromé bezpečnostní agentury.

2.2 Podezřelé chování a jeho monitoring

Cílem monitorování a detekce podezřelého chování je odhalit kriminální čin nejlépe v přípravné fázi. Důležitým faktorem pro monitorování podezřelého chování je preventivní přístup, který je založen na analýze chování. Výsledkem je vyhodnocení situace, která se vymyká standardním situacím, nezapadá do určitého prostředí a příp. představuje reálnou hrozbu.

Detekce podezřelého chování je členěna na tři hlavní oblasti:

- abnormalita v rámci prostředí (technické vybavení prostředí je zcela nepřiměřené okolnímu prostředí),
- podezřelé osoby nezapadající do prostředí (pachatel zjevně nezapadá svým zjevem či chováním do okolního prostředí),
- detaily (pocení, stres).

Pro účely monitorování podezřelého chování je rozlišován i zdroj ohrožení:

- vnější zdroj hrozby (zloděj, útočník),
- vnitřní zdroj hrozby (kmenoví zaměstnanci).

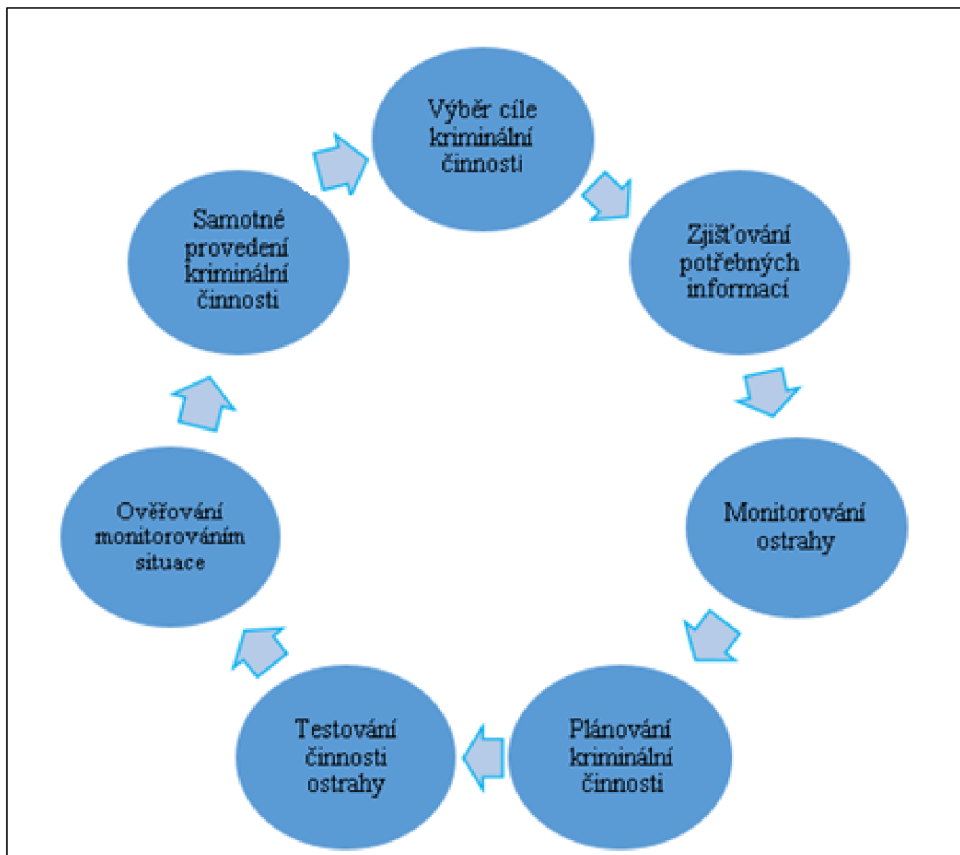
2.2.1 Cyklus před útokem

Samotnému provedení krádeže ve velkoobchodě předchází několik na sebe navazujících logických kroků, které by měly být vodítkem pro ostrahu při odhalování potenciálních pachatelů. Jedná se o několik fází, přičemž jednotlivé fáze na sebe plynule navazují.

Fáze cyklu před útokem:

- 1) V první fázi přípravy na kriminální činnost si pachatel vybere konkrétní cíl, např. krádež alkoholu.
- 2) Druhou fází je zjišťování potřebných informací, kdy si pachatel ověřuje např. přítomnost kamerového systému, resp. fyzickou přítomnost pracovníka fyzické ostrahy.
- 3) V případě, že narazí na prvky ochrany, přichází třetí fáze. V té monitoruje činnost ostrahy, příp. prvky technické ochrany.
- 4) Následně pachatel přechází plynule do čtvrté fáze cyklu, při které si plánuje provedení krádeže.
- 5) V páté fázi je pokus o testování činnosti ostrahy.
- 6) V předposlední fázi si pachatel ještě jednou ověřuje situaci monitorováním, resp. ověřuje a posuzuje vhodnost situace k provedení kriminální činnosti.
- 7) V poslední, sedmé fázi, se pachatel odhodlává k samotnému provedení krádeže.

Schéma fází je zobrazeno na obrázku 2.1.



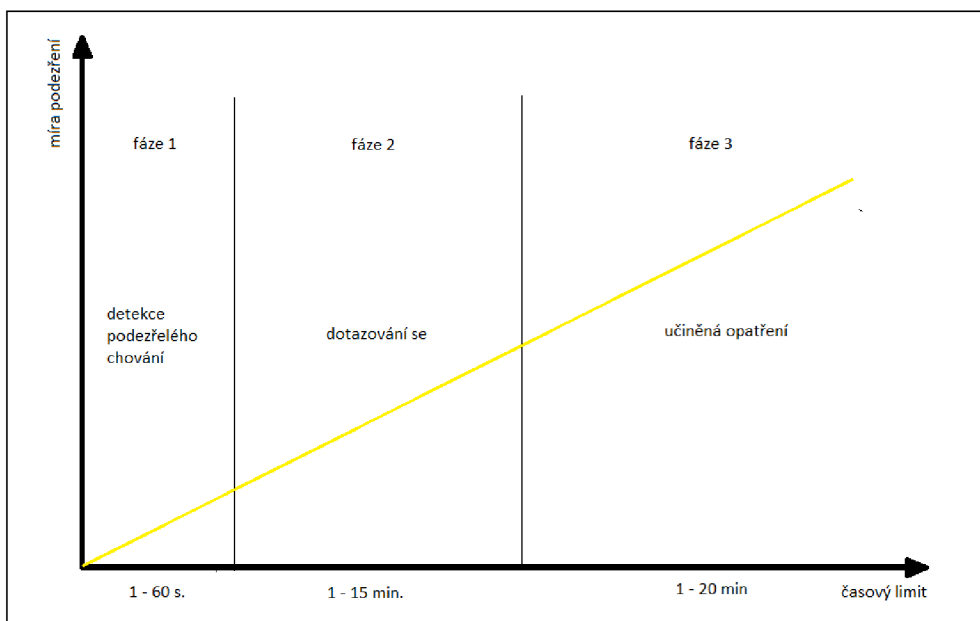
Obr. 2.1 Schéma fází cyklu před útokem

Zdroj: vlastní zpracování.

2.2.2 Detekce podezřelého chování

Dle informací na stránkách MV ČR [18] je metoda detekce podezřelého chování prvkem tzv. proaktivních bezpečnostních opatření. Ta lze charakterizovat tak, že samotný bezpečnostní systém nezůstává neaktivní až do chvíle samotného útoku, ale naopak se snaží podezřelou aktivitu předcházející samotnému útoku co nejdříve identifikovat. Cílem detekce podezřelého chování, resp. podezřelých znaků chování, je aktivní hledání podezřelých znaků, které se vymykají chráněnému prostředí. Jednotlivé znaky jsou pro každé prostředí hledány unikátně, neboť každé prostředí má svá specifika.

Principem detekce podezřelého chování je rozdělení nestandardní situace do tří fází. Každá z fází má předem stanovený časový limit, během kterého se musí osoba rozhodnout a správně vyhodnotit celou situaci. Čím vyšší je míra podezření, tím vyšší je časová náročnost každé fáze. Výsledkem správné detekce podezřelého chování je buď krok dotazování se, nebo adekvátní reakce na nově vzniklou situaci, popř. samotná negace hrozby.



Obr. 2.2 Grafické znázornění fází detekce podezřelého chování

Zdroj: vlastní zpracování.

Detekci podezřelého chování je možné aplikovat do různých podob. V případě prostředí velkoobchodní jednotky lze využít následující kategorie:

- kmenoví zaměstnanci velkoobchodu,

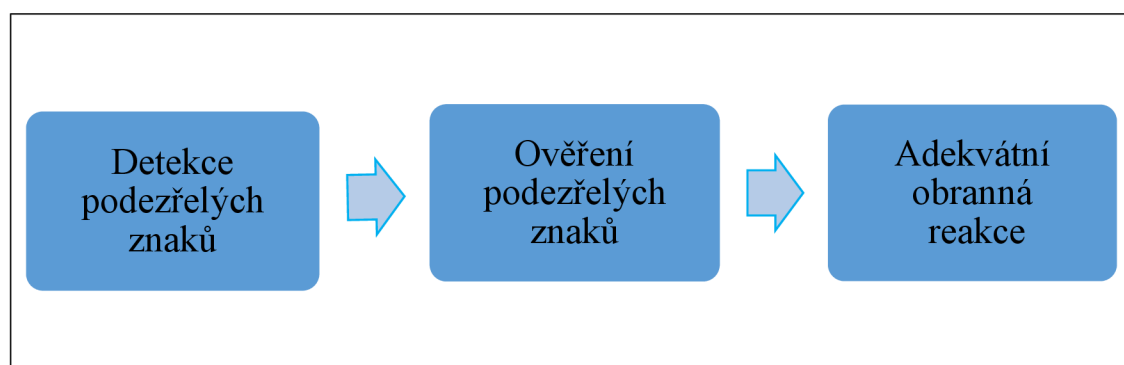
- zaměstnanci úklidové firmy,
- zaměstnanci soukromé bezpečnostní agentury,
- pravidelní odběratelé zboží,
- dopolední návštěvy důchodců, či rodičů (zejména matek) na rodičovské dovolené,
- nárazoví odběratelé zboží,
- bezdomovci,
- promotéři zboží,
- sociálně slabší spoluobčané,
- osoby vyznávající jiná náboženství (sekty apod.).

Smyslem detekce podezřelého chování je stanovení pravidel tzv. normálního chování pomocí bezpečnostních pracovníků. Poté jsou zaměstnanci ostrahy schopni identifikovat případné odchylky. Kvalitně proškolený pracovník ostrahy nemá následně problém bezpečně identifikovat odchylky od normálního režimu a adekvátně reagovat. Nejcennější součástí této bezpečnostní metody je znalost místní rutiny.

2.2.3 Znaky podezřelého chování

Detekce znaků podezřelého chování je pouze prvotní činností, kterou je nutné provést v případě detekce podezřelého chování. Pro rychlou a účinnou ochranu nelze zůstat pouze u odhalení, resp. pojmenování znaků podezřelého chování. Vždy musí následovat adekvátní reakce ze strany bezpečnostního pracovníka. Vhodně zvolená reakce se musí zároveň pružně přizpůsobit situaci dle fáze útoku, kterému znaky odpovídají.

Schematicky lze zobrazit využití detekce podezřelých znaků – viz obrázek 2.3.



Obr. 2.3 Schéma využití detekce podezřelých znaků

Zdroj: vlastní zpracování.

Mezi znaky podezřelého chování pro potřeby pracovníků bezpečnostní agentury pracujících v prostorech velkoobchodní jednotky lze zahrnout:

- pořizování fotografií prostoru velkoobchodní jednotky, příp. pořizování záznamů kamerového zabezpečení, dále pořizování videonahrávek,
- opakovaný výskyt bez nákupu zboží, resp. nákup nezvykle malého množství zboží,
- neobvyklý pohyb ve vnitřních prostorech velkoobchodní jednotky, popř. v prostorech před velkoobchodní jednotkou, častá změna rychlosti chůze,
- úmyslné zahalování se ve snaze ztížit, příp. zcela znemožnit identifikaci osob,
- vyhýbání se jakémukoliv kontaktu s ostrahou, popř. vyhýbání se místům střeženým kamerovým systémem,
- abnormální zjišťování informací od personálu, které se zjevně netýkají sortimentu nabízeného velkoobchodní jednotkou,
- zjevně neadekvátní ošacení, příp. neadekvátní příruční zavazadla (např. speciálně upravená kabelka vystlaná hliníkem pro úmyslné rušení EAS systémů),
- příznaky nadměrného stresu (pocení, třes v hlase, váhání či nerozhodnost).

Ukazatele znaků podezřelého chování lze v reálném případě nejsnadněji rozpoznat za pomoci fyziologických ukazatelů, známých jako ukazatelé stresu. Příznaky nadměrného stresu v sobě skrývají velké množství ukazatelů, které lze poměrně bezpečně a hlavně rychle identifikovat. Zaměstnanec ostrahy se při výkonu své činnosti nemusí zaměřit pouze na základní znaky nadměrného stresu (pocení, váhání), ale měl by naopak vzít v potaz i další ukazatele nadměrného stresu. Přidruženými znaky vhodnými k identifikaci jsou pozorování hodin, přehnané upravování své osoby, resp. kontrolování své osoby, mumlání či šeptání (např. modlení se), vykazování tzv. tunelového vidění, jednání bez emocí či negace příkazů autorit (např. zaměstnance ostrahy).

2.3 Analýza současného stavu technologií a procesů pro monitorování chování zákazníků

Analýza obecně umožňuje dekompozici a zkoumání složitějších skutečností rozkladem na jednodušší, základní celky. Cílem analýzy v této práci je identifikovat podstatné procesy elementárních částí celku, aby bylo možné po zhodnocení analýzy identifikovat problémy, které se stanou předmětem návrhové části práce.

2.3.1 Bezpečnostní systémy a bezpečnostní technologie vybrané velkoobchodní jednotky

Všechny prostory velkoobchodu, včetně jeho technického zázemí a skladovacích ploch, **jsou zabezpečeny jak pomocí elektronických zabezpečovacích systémů (EZS), tak i pomocí elektronických požárních systémů (EPS)**. V případě narušení zastřežených prostor dochází k hlášení na dohledové a poplachové přijímací centrum (DPPC) soukromé bezpečnostní agentury. Zároveň jsou na zabezpečovací systém napojeny nouzové východy velkoobchodu.

V místě objektu je nepřetržitá fyzická ostraha objektu. Ta se pro potřeby denní směny skládá vždy minimálně ze 4 osob. V pracovních dnech je ostraha posílena o jednoho člena. Pro potřeby noční směny jsou přítomni na objektu minimálně 2 členové ostrahy, pro vybrané dny je ostraha posílena o dalšího člena soukromé bezpečnostní agentury. Fyzická ostraha objektu zajišťuje přímou fyzickou obsluhu systémů EZS i EPS.

Dalšími prvky fyzické bezpečnosti jsou **zabezpečení pomocí kamerového systému (CCTV) a ochranné prvky zboží**. Každá pokladna je vybavena tlačítkem tísňového hlášení stejně jako prostory trezoru. Kamerové záznamy sleduje člen ostrahy v kamerové místnosti. Ty lze v případě potřeby využít i pro zpětné dohledávání údajů/dat.

Všechny vstupy do budovy, včetně skladových prostor a služebního vchodu, jsou vybaveny bezpečnostní bránou. Ke vstupu do prodejny slouží přístupový systém na čip, respektive na čárový kód. Tím dochází k eliminaci vstupu nežádoucích osob bez registrace. Služební vchod je vybaven elektronickým turniketem na čipové karty. Pomocí tohoto elektronického turniketu lze zaznamenat všechny průchody

kmenových zaměstnanců, ale i zaměstnanců externích. Jak evidencí vstupu pro zákazníky, tak evidencí vstupu pro zaměstnance se vytváří přehled o pohybu osob uvnitř objektu.

Serverové místnosti v zázemí objektu jsou hlídány za pomoci teplotních čidel. V případě, že by jejich teplota stoupla nad předem určenou hranici, okamžitě se spustí elektronické informační zařízení, a zároveň je také odeslána SMS zpráva na telefon IT správce. **Veškeré síťové aktivní prvky jsou v uzamykatelných síťových skříních** (rack skříních).

2.3.2 Systém Altworx

Systém Altworx je nástrojem, který propojuje a detekuje události v jednotlivých systémech v reálném čase situace, které jsou pro koncového uživatele důležité. Zároveň tyto situace pomáhá řídit. [19]

Tento systém je v konkrétním případě velkoobchodní jednotky využíván k vytváření sdílené databáze podezřelých osob, a zároveň také k přiřazení přístupových karet k těmto osobám. Dle posouzení osoby, která dává vstupní data do databáze, lze přiřadit míru rizika podezřelých osob na tzv. black listu.

I když systém nabízí spoustu přidružených schopností, jako např. monitorování vjezdu za pomoci SPZ či sledování podezřelé osoby v aktuálním čase za pomoci inteligentního kamerového systému, v konkrétním případě velkoobchodní jednotka tyto možnosti aktivně nevyužívá z důvodu absence rozšířeného kamerového systému.

2.3.3 Ochrana lidských zdrojů a osobních údajů

Proti zneužití informací prostřednictvím PC jsou domény chráněny přístupovým heslem. Veškeré databáze jsou zabezpečeny přístupovými hesly, která jsou spjata s pozicemi zaměstnanců. Podle své pozice mají umožněna různá oprávnění. Zároveň nemají uživatelé přístup k instalování jakýchkoliv software na svých PC. Data z provozu PC jsou zálohována do datového centra, dále jsou PC chráněna centrálně ze serveru řízeným antivirem.

Zaměstnanci společnosti jsou od doby zahájení pracovního poměru vázáni mlčenlivostí, která je vyžadována smlouvou. Při ukončení pracovního poměru musí projít přes všechny úseky pro písemné potvrzení, jenž jim prokáže, že nemají žádné další

závazky vůči společnosti ani vůči soukromé bezpečnostní agentuře. Zároveň dojde k blokaci přístupu do interních systémů velkoobchodu a k blokaci všech zaměstnaneckých vstupních karet, které umožňují zaměstnancům nákup u této společnosti.

Zákazníci jsou při registraci seznámeni s pravidly o ochraně osobních údajů, se kterými musí souhlasit. Tento úkon stvrdí svým podpisem. Dále zákazník souhlasí s evidencí svých osobních údajů pro účely registrace. Vše se odehrává v souladu s Obecným nařízením o ochraně osobních údajů (GDPR). Pokud zaměstnanci přijdou do styku s osobními údaji zákazníků, jsou povinni dodržovat schválené pokyny a řídit se jimi u velkoobchodní společnosti pro maximální ochranu takovýchto dat.

2.3.4 Identifikace problémů spojených s monitoringem

Zavedená bezpečnostní opatření v sobě skrývají mnohá úskalí v jejich využívání a v nedokonalosti systému.

V rámci zhodnocení analýzy jsou identifikovány tyto problémy:

- nedostatečný přehled o pohybu osob uvnitř objektu,
- zastaralý kamerový systém pro monitoring,
- nedostatečné pokrytí celého prostoru kamerovým systémem – existence tzv. slepých míst.

Prvotním problémem je možnost vstupu většího počtu zákazníků do prostoru velkoobchodní jednotky na jednu vstupní kartu. Zároveň již dále nelze ověřit, že osoba, jež vstupuje dovnitř prodejny, je opravdu osobou, na níž je karta zaregistrována. Dalším, přidruženým problémem hned při vstupu do prodejny je možnost, kdy po otevření elektronické vstupní brány může dovnitř vstoupit naprosto cizí osoba, která pouze projde s platně registrovaným zákazníkem. Tím se vytrácí přehled o osobách, jež se pohybují uvnitř prodejny.

Zastaralý kamerový systém s nízkou kvalitou obrazu, popř. jeho celková nefunkčnost je velkou hrozbou pro bezpečnostní politiku prodejny. Ostraha prodejny se v případě problému musí potýkat s tím, že díky kvalitě záznamu nelze buď dohledat potřebnou situaci vůbec, nebo popř. jsou tyto materiály neprůkazné (např. pro potřeby Policie České republiky). Je potřeba si uvědomit, že samotné kamerové záznamy mohou sloužit

zároveň pro ochranu zaměstnanců společnosti při řešení jakýchkoliv konfliktních situací.

Na prodejně lze nalézt tzv. slepá místa, která umožňují zákazníkům, ale i zaměstnancům nevhodné chování mimo jakýkoliv záznam.

3 Návrh zefektivnění bezpečnostních procesů a technologií monitoringu

V dnešní době, kdy dochází k neustálému rozvoji ochranných systémů, je stávající ochrana zboží proti krádežím v prostředí velkoobchodu v některých případech nevyhovující a nedostatečná. Je nezbytně nutné implementovat ochranné systémy proti krádeži zboží.

Bezpečnostní manažer obchodní jednotky musí správně posoudit náklady spojené se samotnou implementací, resp. modernizací bezpečnostních systémů a následným provozem bezpečnostních systémů při zohlednění počtu krádeží, resp. škodou vzniklou krádežemi. Obecně jsou náklady na bezpečnostní systém při zohlednění možných škod na relativně nízké úrovni.

Pro zvolení vhodného návrhu zefektivnění bezpečnostních procesů a technologií je nutné přesně analyzovat stávající bezpečnostní opatření velkoobchodu, konkrétně kamerového systému, fyzické ostrahy a zabezpečení pomocí pevných bezpečnostních prvků. Podle zjištěného stavu následně vhodně navrhnout modernizaci bezpečnostních opatření.

Z bezpečnostních důvodů konkrétního popisu bezpečnostního systému velkoobchodní jednotky nelze přesně specifikovat, o kterou provozovnu velkoobchodní jednotky se jedná. Popisované informace vychází z reálného stavu velkoobchodní jednotky a byly zjištěny ve spolupráci s bezpečnostním manažerem společnosti.

3.1 Zhodnocení analýzy stávajícího kamerového systému

Kamerový systém slouží v prostoru velkoobchodní jednotky k prevenci při zajištění bezpečnosti celého objektu, dále pro potřeby dohledávání zboží v sekci distribuce. Provozování kamerového systému je bez souhlasu vstupujících osob, neboť pořizované záznamy nejsou pořizovány pro účely zpracování osobních údajů. Záznamy jsou uchovávány v rozmezí 2 – 3 měsíců dle kapacity úložiště. Poté jsou automaticky vymazány. O zpřístupnění uchovaných záznamů mohou písemnou formou zažádat pro účely šetření trestné činnosti oprávněné subjekty, např. Policie ČR. Velkoobchodní jednotka informuje osoby vstupující do jejich prostor o využívání kamerového systému

nálepkou umístěnou u hlavního vstupu i na dalších místech objektu – Objekt je monitorován kamerovým systémem.

Stávající kamerový systém je složen ze dvou rozdílných soustav. Aktuální počet kamer využívaných pro monitorování bezpečnostní situace velkoobchodu činí 105 kusů. Ty jsou přenášeny na 12 monitorů umístěných v kamerové místnosti velkoobchodu. Na objektu převažují starší analogové kamery, které jsou postupně nahrazovány digitálním kamerovým systémem. Tento systém je v dnešní době již zastaralý a nevyhovující. Jak je uvedeno výše, v prostorech velkoobchodu se bohužel nachází i tzv. slepá místa, která nejsou v zorném poli žádné kamery.

3.1.1 Analogový kamerový systém

Z celkového počtu 105 kamer je 82 kamer staršího analogového typu. Kamerový systém je používán v režimu kamerového systému se záznamy. Kamery snímají prostor nejen uvnitř velkoobchodu, ale kamery jsou umístěny i v perimetru budovy a v prostoru parkoviště. Zde jsou mimo jiné pro účely monitorování okolí. Obraz je přenášen na 10 monitorů. Nejčastěji je přenos obrazu na každém monitoru nastaven na 16 kamer.

Vzhledem ke špatné kvalitě obrazu má pracovník bezpečnostní služby ztížené podmínky při zajišťování ochrany objektu, včetně potřeb dohledávání. Část kamer původního analogového typu po modernizaci na IP kamery jsou využívány jako atrapy.

3.1.2 Digitální kamerový systém

Zbývajících 23 kamer je již modernizováno na IP kamery. Kamerový systém je využíván v režimu kamerového systému se záznamy. Kamery snímají prostor pokladní zóny a oblast východu, dále prostory distribuce umístěné v zázemí velkoobchodu. Obraz digitálních kamer je přenášen na 2 monitory. Na jednom monitoru je nastaveno zobrazení 11 kamer, na druhém monitoru je nastaveno zobrazení 12 kamer.

Jelikož se jedná o modernizované digitální kamery, je kvalita obrazu nesrovnatelně vyšší v porovnání s původním analogovým systémem. Digitální kamerový systém využívají pracovníci bezpečnostní soukromé služby často pro dohledávání reklamací, příp. při kontrole práce zaměstnanců pokladen.

3.2 Zhodnocení analýzy stávající fyzické ostrahy

Fyzickou ostrahu velkoobchodu provádějí vyškolení pracovníci soukromé bezpečnostní agentury. Důležitost fyzické ostrahy lze doložit vyjádřením autorů Doucek a kol. [20], že zajištění bezpečnosti je důležitou součástí také z hlediska lidských zdrojů. Často bývá nazýváno personální bezpečností. Základním faktorem bezpečnosti z hlediska lidských zdrojů je potřeba přesné definice a následná dokumentace bezpečnostních rolí a odpovědností.

Služba fyzické ostrahy je zajištěna i v době, kdy je prostor velkoobchodu uzavřen pro veřejnost, včetně svátků. Fyzická ostraha slouží také jako vrátnice velkoobchodu. V případě mimořádných událostí slouží také jako ohlašovna požáru.

Nejvyšší nedostatek z hlediska bezpečnosti lze spatřit ve fyzické ostraze. Vzhledem k velikosti velkoobchodu, včetně parkoviště, a zároveň k požadavkům klienta na fyzickou ostrahu považují stávající počet bezpečnostních pracovníků za nedostatečný. Při aktuálním počtu bezpečnostních pracovníků nelze pokrýt všechna stanoviště. Strážníci musí odbíhat na jiná pracoviště, kde chybí další pracovníci bezpečnostní služby. V tu chvíli je nestřežená původní pozice ostrahy.

3.2.1 Úkony pracovníků soukromé bezpečnostní služby

Úkony jednotlivých pracovníků jsou rozděleny dle jejich pozice pracovního zařazení. Fyzická ostraha je složena z pozice vedoucího objektu, vedoucího denní i noční směny, pracovníka ostrahy distribuce, pracovníka ostrahy pokladní zóny a parkoviště a v poslední řadě z pracovníka zajišťujícího potřeby služebního vchodu.

V současné době je celkový počet pracovníků bezpečnostní agentury cca 25 osob. S ohledem na požadavek nepřetržité ostrahy některých stanovišť není možné poskytnout plnohodnotnou službu klientovi. Pracovní doba zaměstnanců je dle stanovišť buď 8 hodin, nebo 12 hodin.

3.2.1.1 Vedoucí objektu

Pracovník na pozici vedoucí objektu zodpovídá za své podřízené pracovníky ostrahy i za celkovou bezpečnostní situaci na objektu. Je kontaktní osobou s bezpečnostním

manažerem velkoobchodu i bezpečnostními složkami, např. v případě žádosti o poskytnutí kamerových záznamů Policií ČR.

Mezi povinnosti tohoto pracovníka patří kontrola všech stanovišť, včetně ústrojové kázně zaměstnanců ostrahy, zaškolení nových zaměstnanců, nápomoc zaměstnanci na pozici vedoucího směny, nepřetržitá telefonní pohotovost, kontrola a vedení klíčového režimu, zajištění dokumentace. Vedoucí objektu také zodpovídá za personální stránku ostrahy. Pro vedení společnosti reportuje pravidelně každý měsíc aktuální informace týkající se bezpečnostní stránky velkoobchodu. V poslední řadě provádí vyhodnocení kamerových záznamů, včetně kontroly zaměstnanců velkoobchodu.

3.2.1.2 Vedoucí směny

Vedoucí směny zakládá a kontroluje správnost vedené administrace, provádí obsluhu kamerového systému, příp. přidružených zařízení elektronické ochrany objektu v kamerové místnosti objektu, provádí zabezpečení zboží pevnými bezpečnostními prvky, dále vykonává obchůzkovou kontrolní činnost v prostorech velkoobchodu. Fyzicky odemyká i uzamyká velkoobchod. V případě absence vedoucího objektu zajišťuje jeho zástup.

Pracovník na této pozici má největší množství pracovních povinností během své služby. Tu není možné kvalitně vykonávat pouze jedním zaměstnancem. V případě, že dojde k absenci pracovníka ostrahy na jiné pozici, nahrazuje vedoucí směny tuto pozici svou osobou.

3.2.1.3 Pracovník ostrahy distribuce

Pracovník ostrahy distribuce dohlíží na výdej i příjem zboží přes distribuci, kontroluje a eviduje stav obalových materiálů. Provádí namátkové kontroly vychystaného zboží. Je podporou při plnění pracovních povinností vedoucího směny.

Ostraha není přítomna na distribuci nepřetržitě. V takovém případě je nutnost využít pracovníka vedoucího směny, popř. vedoucího objektu. Problémem je časová prodleva, která nastává dobou příchodu jiného zaměstnance ostrahy, zároveň původní stanoviště zůstává bez ostrahy.

3.2.1.4 Pracovník ostrahy pokladní zóny a parkoviště

Tento pracovník provádí kontrolní činnost nad pracovníky pokladní zóny velkoobchodu. Monitoruje a vyhodnocuje bezpečnostní situaci na přidruženém parkovišti velkoobchodní jednotky. V případě, že dojde ke zjištění krádeže, je připraven zasáhnout proti pachateli krádeže v prostoru pokladní zóny. Při aktivaci EAS systémů provádí nezbytné úkony spojené s kontrolou osob i zboží, resp. zakoupeného zboží.

Bezpečnostní hrozba nastává ve chvíli, kdy pracovník ostrahy monitoruje prostor parkoviště, příp. provádí manipulaci s vozíky, resp. jejich úklid. Pokud by ve stejnou chvíli došlo k aktivaci EAS systémů, není možné provést kontrolu a případný pachatel může opustit prostor velkoobchodu bez kontroly.

3.2.1.5 Pracovník ostrahy služebního vchodu

Pracovník vykonává obsluhu klíčového režimu, obsluhu elektronického zabezpečovacího systému, včetně požárního systému a obsluhu vjezdu do zázemí areálu. Dále provádí výstupní kontrolu zaměstnanců a vede docházku. V případě opatření na COVID-19 prováděli pracovníci ostrahy služebního vchodu i nezbytné úkony (např. měření teploty).

V případě zajišťování kontroly zaměstnanců při průchodu služebním vchodem nelze dosáhnout požadované kvality kontroly, jelikož pracovník služebního vchodu musí zároveň vykonávat jiné činnosti. Kvalita kontroly je také ovlivněna kontrolou opačného pohlaví.

3.3 Zhodnocení analýzy stávající ochrany za pomoci pevných bezpečnostních prvků

Pro zabezpečení zboží před krádeží využívá velkoobchod pevné bezpečnostní prvky. Samotné zabezpečení zboží proti krádeži provádí zaměstnanci ostrahy. V současné chvíli disponuje velkoobchodní jednotka 5 kotouči jednorázových měkkých etiket, každá z rolí obsahuje 1 000 kusů. Tvrdých etiket je k dispozici přibližně 400 kusů, bezpečnostních obalů zhruba 130 kusů. Pro zabezpečení drahého alkoholu je k dispozici 19 speciálních etiket. V případě plastových etiket je k dispozici cca 800 kusů. Pro účely zabezpečení zboží pomocí bezpečnostních lanek je k dispozici 37 kusů. K zabezpečení

elektroniky a domácích potřeb je k dispozici zaměstnancům ostrahy okolo 80 kusů smyčkové ochrany.

3.4 Návrh pro nastavení bezpečnostních procesů za účelem zefektivnění monitoringu

Cílem vlastního návrhu zefektivnění je navrhnout taková bezpečnostní opatření, která minimalizují nejvyšší rizika nepřipustného chování zákazníků. Všechna tato opatření je potřeba zohlednit i z hlediska logistických procesů tak, aby byly nastaveny bezpečnostní procesy s co nejvyšší mírou efektivity.

3.4.1 Modernizace kamerového systému

V této části je popsán návrh na modernizaci kamerového systému jak pro využití střežení vnějšího prostoru, tak pro využití střežení vnitřního prostoru. Kamery jsou navrženy především za účelem zvýšení ochrany osob a majetku, monitorování přepravy finančních prostředků i jako prevence proti vandalismu. Dále považuji za vhodné využití kamerového systému pro monitorování dopravní situace na parkovišti v případě dopravní nehody, popř. provozování podomního prodeje.

Modernizace kamerového systému je navržena prostřednictvím kamer od výrobce Dahua, kdy se jedná o velmi kvalitní zařízení. Digitální kamery disponují velkým množstvím individuálního nastavení i příslušenstvím vhodným pro velkoobchod. To vše za přijatelné cenové nabídky.

S ohledem na konkrétní potřeby velkoobchodu monitorování perimetru objektu, včetně přilehlého okolí ve svém návrhu uvádím i využití kompaktních mini hybridních termokamer. Ty v poslední době nahrazují stále častěji původní infrakamery, jelikož nejsou zatíženy vlivem počasí. Tím je dosažena eliminace falešných poplachů.

Pro účely využití kamerového systému je zřízená speciální místnost, která má nepřetržitý provoz a je obsazena nejméně jedním vyškoleným pracovníkem ostrahy. Nutnost zajištění nepřetržitého provozu kamerové místnosti je dána povinností vyplývající z požární bezpečnosti.

3.4.1.1 Kompaktní mini hybridní termokamera

Jako vnější ochranu objektu navrhuji využití termokamer v provedení typu Dahua TPC-BF1241-D3F4, které jsou vybaveny rozlišením viditelného spektra 4 Mpx, Smart IR LED dosvitem až 30 m., inteligentní funkcí ochrany perimetru a dalšími prvky.



Obr. 3.1 Ilustrační obrázek IP termokamery

Zdroj: [21].

Základní parametry IP termokamery jsou uvedeny v následující tabulce.

Tab. 3.1 Základní parametry navržené IP termokamery

Základní parametry- Dahua TPC-BF1241-D3F4	
Typ technologie	IP kamera
Prostředí	exteriér
Rozlišení	4 Mpx
Napájení	12 V DC, PoE
Stupeň krytí	IP 67
IR přísvit	až 30m
Maximální rozlišení termovize	256 x 192 px
Maximální snímková rychlost termovize	25 fps @ 256 x 192 px
Objektiv termovize	3,5 mm
Objektiv	4 mm
Maximální rozlišení	2336 x 1752 px
Maximální snímková rychlost	25 fps @ 2336 x 1752 px
Spotřeba	< 14 W
Inteligentní funkce	detekce osob a vozidel
Rozměry	205,5 x 90,4 x 90,1 mm
Pracovní teplota	od - 30°C do + 60°C
Hmotnost	0,9 kg

Zdroj: [21].

3.4.1.2 Kompaktní IP kamera vnitřní

Pro vnitřní instalaci kamer navrhuji kameru v provedení typu Dahua IPC-HFW5541E-ZE-27135 5, která je vybavena rozlišením viditelného spektra 5 Mpx, Smart IR LED přísvitem až 50 m., motorickým zoomem, krytím IP 67 a dalšími prvky.

Pro zvolení této konkrétní kamery jsem se rozhodl s ohledem na její vyšší schopnost rozlišení obrazu, kdy je prostor velkoobchodu rozsáhlý a v případě potřeby dohledání pachatelů krádeží je potřeba detailní rozlišení při krádeži zboží. Dále považuji za vhodné využití její funkce IR LED přísvit s dosahem až 50 m, kdy jsou kamery instalovány i v zázemí velkoobchodu, kde se pohybují zaměstnanci, a to jak v denním, tak v nočním režimu provozu.



Obr. 3.2 Ilustrační obrázek vnitřní IP termokamery

Zdroj: [22].

Tab. 3.2 Základní parametry navržené vnitřní IP termokamery

Základní parametry- Dahua IPC-HFW5541E-ZE-27135 5	
Typ technologie	IP kamera
Prostředí	interiér
Rozlišení	5 Mpx
Napájení	12 V DC, 908 Poe, ePoe
Stupeň krytí	IP 67
IR přísvit	až 50m
Zoom	2,7 – 13,5 mm
Úhel záběru	100°- 28°
Maximální rozlišení	2592 x 1944 px
Maximální snímková rychlost	20 fps @ 2592 x 1944 px
Slot na MicroSD kartu	max. 256 GB
Inteligentní funkce	zachycení obličeje, videoanalýza
Rozměry	205,5 x 90,4 x 90,1 mm
Pracovní teplota	od - 30°C do + 60°C
Hmotnost	1,11 kg

Zdroj: [22].

3.4.1.3 PTZ IP kamera vnitřní

Pro doplnění kamerového systému využitého pro vnitřní instalaci kamer navrhuji kameru v provedení typu Dahua SD42C212T-HN-S2 2, která je vybavena rozlišením viditelného spektra 2 Mpx, mechanickým IR filtrem, motorickým zoomem, krytím IK 10 a jiným.

Pro zvolení této kamery jsem se rozhodl jako vhodné doplnění střežení větších prostorů velkoobchodu s nižšími nároky na kvalitu rozlišení přenášeného obrazu. Typickým příkladem takto střeženého prostoru jsou jednotlivé úseky velkoobchodu pro přehledné zobrazení aktuální situace pracovníkem ostrahy.



Obr. 3.3 Ilustrační obrázek PTZ IP kamery

Zdroj: [23].

Tab. 3.3 Základní parametry navržené PTZ IP kamery

Základní parametry- Dahua SDC42C212T-HN-S2 2	
Typ technologie	IP kamera
Prostředí	interiér
Rozlišení	2 Mpx
Napájení	vlastní zdroj
Stupeň krytí	IK 10
IR přísvit	mechanickým filtrem
Zoom	5,3 – 64 mm
Úhel záběru	58,2°- 4,8°
Maximální rozlišení	1920 x 1080 px
Maximální snímková rychlost	25 fps @ 1920 x 1080 px
Slot na MicroSD kartu	max. 128 GB
Inteligentní funkce	zachycení obličeje
Rozměry	ø 198 x 158 mm
Pracovní teplota	od - 30°C do + 60°C
Hmotnost	2,3 kg

Zdroj: [23].

3.4.1.4 Návrh rozvržení kamerového systému

Z bezpečnostního hlediska není možné veřejně prezentovat aktuální rozvržení kamerového systému velkoobchodní jednotky. Pro modernizaci kamerového systému navrhuji zachovat stávající rozložení kamerového systému, kdy dojde pouze k nahrazení starého a nevyhovujícího analogového kamerového systému digitálním kamerovým systémem. Zároveň navrhuji v případě velkoobchodu zachovat stávající IP kamery v prostoru distribuce i pokladní zóny.

3.4.1.5 Cenová kalkulace modernizace kamerového systému

Cenová kalkulace je zpracována po odborné konzultaci na základě obecných informací se zástupcem dodavatelské firmy a má pouze informativní charakter s ohledem na možnost změny požadavků.

Platnost cenové kalkulace je omezená, platí maximálně po dobu 3 měsíců od data zpracování a uveřejnění cenové kalkulace. S ohledem na aktuálně nepříznivý vývoj cen na trhu je nutné před samotnou realizací ověřit u dodavatelské firmy dostupnost všech aktivních prvků i komponentů. Zároveň je třeba brát ohled na možné prodloužení dodací lhůty jednotlivých komponentů.

Cenová kalkulace modernizace je zpracovaná a uvedena v příloze A. Celková výše modernizace kamerového systému činí 2 001 094,- Kč bez DPH.

3.4.2 Úprava režimu fyzické ostrahy

Při úpravě režimu fyzické ostrahy je brán v úvahu nedostatek zaměstnanců na pozici pracovník ostrahy. Dojde-li k zajištění dostatečného počtu vyškolených pracovníků ostrahy, dojde k eliminaci chybovosti vlivem únavy, zároveň ke zkvalitnění samotné činnosti na jednotlivých stanovištích. V případě zjištění páčání trestné činnosti bude zaměstnanec ostrahy připraven adekvátně zasáhnout vůči pachateli.

Zaměstnance ostrahy je potřeba adekvátně motivovat při jejich práci, ať už dostatečným finančním ohodnocením, tak benefity poskytovanými zaměstnavatelem. Zároveň je nezbytné provádět další odborná školení zaměstnanců ostrahy.

3.4.2.1 Navýšení fyzické ostrahy

S ohledem na velikost velkoobchodní jednotky i na požadovanou činnost na jednotlivých stanovištích navrhuji navýšení pracovníků ostrahy pro účely fyzické ostrahy velkoobchodu alespoň o další dva pracovníky ostrahy. Tento počet považuji za naprosto nezbytné minimum.

Pracovník na pozici ostrahy parkoviště

Ve chvíli, kdy by byla navýšena kapacita pracovníků ostrahy, lze vytvořit samostatnou pozici pro pracovníka ostrahy parkoviště. Důvodem k vytvoření této pozice je nutnost nepřetržité přítomnosti zaměstnance ostrahy pokladní zóny, kdy tento pracovník nemůže zároveň provádět doplňkovou činnost v prostorech parkoviště. Z bezpečnostního hlediska představuje stávající řešení velkou bezpečnostní hrozbu.

Pracovník by zabezpečoval jak monitorování prostoru parkoviště, včetně vchodů a východů velkoobchodní jednotky, tak i úklid vozíků na parkovišti. V případě, že by došlo ke zjištění krádeže ve velkoobchodu (ale i jakékoliv jiné mimořádné události), může být tento pracovník nápomocen ostatním členům ostrahy.

Pracovník na pozici detektiv prodejny

Druhou pozicí, kterou navrhuji pro zvýšení bezpečnosti, je pracovník na pozici detektiv prodejny. Ten se odlišuje svou činností od strážného obchodu svou vyšší kvalifikovaností i zkušeností. Zároveň provádí kontrolní činnost v civilním ošacení. Pachatel má následně pocit, že osoba vykonávající funkci detektiva prodejny je obyčejným zákazníkem provádějícím nákup. S ohledem na stále se zvyšující počet krádeží v obchodech vnímám činnost detektiva prodejny velmi kladně.

Ve svém návrhu na navýšení ostrahy by došlo k celkovému navýšení strážní služby celkem o 26 hodin denně. Konkrétně by se jednalo o 13 hodin denně v případě pracovníka ostrahy parkoviště, dále o 13 hodin denně v případě pracovníka ostrahy na pozici detektiv prodejny. Jelikož je provoz velkoobchodu i o víkendu, navrhuji navýšení ostrahy i na tyto dny.

3.4.2.2 Cenová kalkulace navýšení fyzické ostrahy

Návrh cenové kalkulace byl zpracován ve spolupráci s finančním oddělením vybrané soukromé bezpečnostní agentury. Tato agentura zastupuje jedno z předních míst

na českém trhu komerční bezpečnosti. Cenová kalkulace vychází z reálných hodnot, které by byly v případě žádosti navýšení ostrahy ze strany klienta navrženy ze strany soukromé bezpečnostní agentury.

Požadavky na profesní vzdělání i samotné zkušenosti na pozici detektiva prodejny jsou vyšší než profesní nároky na pozici strážného prodejny. Z tohoto důvodu je nutné vzít v potaz vyšší náklady na pozici detektiva. Návrh cenové kalkulace vychází ze situace v době psaní diplomové práce. Cena je uvedena bez DPH.

Cenová kalkulace na navýšení fyzické ostrahy je zpracovaná a uvedena v příloze B. Cenový návrh na navýšení fyzické ostrahy činí 132 600,- Kč bez DPH měsíčně. Předpokládaný náklad spojený s navýšením fyzické ostrahy činí 1 591 200,- Kč bez DPH za 1 rok.

3.4.3 Navýšení pevných bezpečnostních prvků

V současné době se zaměstnanci ostrahy potýkají s velkým nedostatkem pevných bezpečnostních prvků. Vzhledem ke značnému množství nabízeného sortimentu je třeba vzít v úvahu navýšení pevných bezpečnostních prvků.

Mohlo by se zdát, že velkoobchod disponuje dostatečným množstvím jednorázových měkkých etiket. Jak už název napovídá, tento ochranný prvek lze použít jen jednou. Tím narůstá finanční nákladnost zabezpečení zboží pomocí tohoto prvku. V případě jednorázových měkkých etiket nenavrhují navýšení počtu.

Opačná situace nastává u pevných bezpečnostních prvků, které lze využít opakovaně. Typickým příkladem jsou krádeže alkoholických nápojů. Ty lze proti krádežím zabezpečit buď pomocí speciálních etiket, nebo pomocí plastových etiket. Ačkoliv by se mohlo zdát, že přibližně 800 kusů bude dostačujících, z pohledu praktické stránky lze tento fakt zcela vyloučit.

Abych si své tvrzení ověřil a mohl se o něj opřít, provedl jsem průzkum zabezpečeného a nezabezpečeného zboží velkoobchodní jednotky. Výsledek je popsán v následující tabulce. Dle výsledků svého průzkumu jsem následně navrhl konkrétní počet navýšení vzhledem ke stávajícímu počtu bezpečnostních prvků.

3.4.3.1 Konkrétní návrh

Pro přehlednost uvedu ve svém návrhu navýšení u každého pevného bezpečnostního prvku zvlášť. V tabulce 3.4 je v prvním sloupci uveden druh bezpečnostního prvku, aktuální počet bezpečnostních prvků je uveden ve druhém sloupci, návrh na navýšení je uveden ve sloupci třetím.

Tab. 3.4 Přehled navýšení pevných bezpečnostních prvků

Navýšení pevných bezpečnostních prvků		
Druh bezpečnostního prvku	Současný stav	Plánovaný stav
Jednorázová měkká etiketa	5 000 ks	5 000 ks
Tvrdá etiketa	400 ks	600 ks
Bezpečnostní obal	130 ks	250 ks
Speciální etiketa	19 ks	19 ks
Plastová etiketa	800 ks	1 500 ks
Bezpečnostní lanka	37 ks	237 ks
Smyčková ochrana	180 ks	400 ks

Zdroj: vlastní zpracování.

Jednorázová měkká etiketa – náklady spojené s využitím jednorázového bezpečnostního prvku nepovažuji za adekvátní ve srovnání s jinými bezpečnostními prvky, které lze použít k zabezpečení zboží opakovaně. Tento bezpečnostní prvek využívá velkoobchod k zabezpečení tabákového zboží a jeho spotřeba není příliš vysoká. V případě, že budou využity všechny jednorázové měkké etikety, doporučuji doplnění do stávajícího stavu.

Tvrdá etiketa – textil a obuv je prodávána ve velkoobchodu pouze jako sezónní zboží. Pro tyto účely by stávající počet tvrdých etiket byl zcela dostatečný. Velkoobchod tímto prvkem ale zabezpečuje i drobnou elektroniku či drogerii. Zde už stávající počet prvků není dostatečný.

Bezpečnostní obal – nedostatek bezpečnostních prvků pro zabezpečení zboží v sekci drobné elektroniky. Často nezabezpečené jsou paměťové karty, USB flash disky, náplně do tiskáren. Konzultací se zaměstnanci ostrahy velkoobchodu jsem zjistil, že problémem při zabezpečení náplní do tiskáren je absence dostatečného počtu větších bezpečnostních obalů, do kterých by se náplně mohly umístit.

Speciální etiketa – nejdražší prémiový alkohol je uzamčen ve skleněné vitríně. Její kapacita ale není dostatečná a další dražší alkohol se nachází i volně v regálech. Ve svém návrhu nedoporučuji navýšení počtu speciálních etiket, jelikož sortiment alkoholu lze dostatečně zabezpečit i pomocí plastových etiket, které jsou ekonomičtější variantou.

Plastová etiketa – největší nedostatek bezpečnostních prvků jsem zjistil při zabezpečení sortimentu alkoholických nápojů. V současném stavu je zabezpečen alkohol zhruba z jedné poloviny. Ve svém průzkumu jsem vzal v potaz pouze alkoholické nápoje s prodejní cenou vyšší než 499,- Kč bez DPH. Zaměstnanci ostrahy několikrát denně prochází prostor pokladní zóny a sbírají plastové etikety, které zůstávají po prodaném zboží. Následně zabezpečují další sortiment alkoholu.

Bezpečnostní lanka – zjištěný nedostatek ochranného prvku, kdy bezpečnostní lanka využívá velkoobchod k zabezpečení elektroniky. Jejich využití není tak časté, jako jiné bezpečnostní prvky, ale v době provádění průzkumu byly využity všechny prvky. Z tohoto důvodu navrhuji navýšení o 200 kusů.

Smyčková ochrana – s velkým nedostatkem smyčkové ochrany se potýkají zaměstnanci ostrahy v případě jejího využití u sortimentu elektroniky, dále kuchyňského náčiní a vybavení, v případě prodeje dražšího masa či nabízeného sezónního zboží. Z rozhovoru s ostrahou prodejny jsem zjistil, že krádeže masa tvoří velkou část odcizeného zboží, ale nemají prostředky pro jeho zabezpečení.

3.4.3.2 Cenová kalkulace navýšení bezpečnostních prvků

Návrh cenové kalkulace jsem zpracoval na základě nabídky firmy ORIS shop, která nabízí všechny navrhované bezpečnostní prvky. Cenová kalkulace vychází z konkrétní nabídky v době psaní diplomové práce. Cena je uvedena bez DPH.

Cenová kalkulace navýšení bezpečnostních prvků modernizace je zpracovaná a uvedena v příloze C.

Cenová kalkulace navýšení pevných bezpečnostních prvků činí 124 860,- Kč bez DPH. Investice nutná na pořízení bezpečnostních prvků je jednorázová, revize aktuálního počtu bezpečnostních prvků by měla být provedena 1 x ročně.

3.5 Riziko selhání RFID systému

Riziko, že RFID systém selže, lze spatřit jak v chování lidí, tak také v možnosti selhání vlastností systému. Z údajů dostupných ze statistického úřadu vyplývá, že se přibližně jeden z patnácti zákazníků pokusí při nákupu v obchodních jednotkách odcizit nějaké zboží.

Pachatelé krádeží se při krádeži zboží snaží systém obejít a využívají přitom znalosti o technických nedostatcích systému. Nejčastější případy snahy provést krádež v obchodě jsou v době, kdy se v obchodě nachází větší počet zákazníků. Zaměstnanci ostrahy nemohou kontrolovat všechny zákazníky najednou. Také mají své další povinnosti a na tuto činnost mají menší prostor. Prostředí velkoobchodu se tak stává častým terčem zlodějů.

Lze konstatovat, že fungující RFID systém má i psychickou roli a dobře funguje při odstrašení nepoctivých zákazníků. Zákazník obchodu se záměrem krást raději navštíví obchod, kde RFID systém je buď nefunkční, popř. zcela schází. Riziko odhalení se tím úměrně snižuje. Z tohoto důvodu je potřeba, aby pracovníci ostrahy pravidelně prováděli kontrolu RFID systému velkoobchodu. Vhodné je provádět kontrolu jedenkrát za den.

Metody, které nepoctivci využívají při obcházení RFID systému, jsou následující: použití rušičky radiového pásma RFID systému, použití kleští či nůžek, využití silného magnetu a případně samotná destrukce bezpečnostních etiket.

Odstínění RFID systému – nejčastější způsob pachatele při snaze obejít bezpečnostní systém. Pokud je zboží zabezpečeno RFID tagem, stačí jakýmkoliv způsobem odstínit radiové vlny. Následně dojde k negaci jeho čitelnosti pomocí detekční brány a pachatel může opustit velkoobchod bez obavy ze zákroku fyzické ostrahy.

Typickým příkladem jsou tašky či kabelky upravené speciálně pro potřebu odstínění. Ty jsou vyplněny mnoha vrstvami alobalu tak, aby došlo k odstínění radiové vlny. Pachatelé ale nepoužívají pouze příruční zavazadla. Pomocí více vrstveného alobalu jsou schopni využít pro odstínění RFID tagů svůj oděv, resp. jeho kapsy.

Pracovník ostrahy není v podstatě schopen sám zjistit využití tohoto způsobu. Aby se zabránilo krádeži zboží ve speciálně upravené tašce, resp. oděvu, je potřeba vybavit detekční brány systémem na detekování alobalu. Zachytí-li detekční brána při průchodu

zákazníka přítomnost alobalové vycpávky, upozorní na to pomocí stroboskopického světla v kombinaci s akustickou signalizací.



Obr. 3.4 Alobalové odstínění umístěné v kabelce

Zdroj: vlastní zpracování.

Rušení rádiového pásma – pracuje na základě vysílání signálu na stejné vlnové frekvenci, kterou využívá i RFID systém. Pokud se spustí rušička rádiového pásma, dojde buď ke snížení účinnosti bezpečnostního systému, nebo k jeho úplnému vyřazení z provozu. Rušička využívá principu, při kterém nelze používat jiná zařízení, která pracují na stejné frekvenci, a zároveň jsou v jejím dosahu. Dosah rušičky rádiového pásma je ovlivněn mnoha faktory. Kapesní rušičky využívané ve velkoobchodu mají velikost srovnatelnou s mobilním telefonem a mají dosah v rozmezí 5 – 15 metrů. V ideálních podmínkách otevřeného prostřanství je teoreticky možné dosáhnout rušení až do vzdálenosti 30 metrů.



Obr. 3.5 Rušička rádiového signálu

Zdroj: [24].

Kleště – častým způsobem při snaze obcházení RFID systému je využití kleští, příp. nůžek na drát. Pomocí nich dokáže pachatel okamžitě mechanicky odstranit bezpečnostní etiku ze zboží. Tím se stává zboží nechráněné a pachatel může opustit prodejnu i s odcizeným zbožím bez povšimnutí.



Obr. 3.6 Boční štípací kleště

Zdroj: [25].

Magnet – pro odstranění pevných etiket využívají pachatelé výkonné magnety, které umísťují např. do příručních zavazadel, popř. do kapes oděvu. Výkonný magnet následně využijí pro neoprávněné odstranění bezpečnostních etiket ze zabezpečeného zboží.

Účinnou ochranou prodejen je využití systému na detekci výkonných magnetů. V případě zjištění přítomnosti silných magnetů upozorní systém personál ostrahy. Systém dokáže upozornit na přítomnost silných magnetů do vzdálenosti zhruba 1 metru po obou stranách čidla. Vhodným umístěním je vchod do prodejny velkoobchodu.

Destrukce RFID etikety – nejméně sofistikovaným způsobem při obcházení RFID systému je fyzická destrukce měkkých etiket. Poškození, popř. úplné odstranění měkkých etiket ze zboží způsobí nečinnost při průchodu detekční bránou. Zničení či odstranění bezpečnostních etiket je druhým nejčastějším způsobem, jakým pachatelé bezpečnostní systém obcházejí.

4 Vyhodnocení přínosů návrhu

V poslední kapitole jsou uvedeny přínosy konkrétních navrhovaných opatření. Za pomoci návrhu bezpečnostních opatření se podařilo splnit hlavní cíl práce, ale i několik přidružených cílů, které jsou zrekapitulovány v této kapitole.

Návrhy uvedené ve 3. kapitole jsou zpracovány za účelem zefektivnění monitoringu podezřelého chování zákazníků s využitím bezpečnostních procesů a technologií.

V minulém roce došlo dle dostupných statistik Policie ČR [26] celkem k 1 089 krádežím vloupáním na celém území ČR. Krádeží v obchodech je evidováno celkem 5 725 na území ČR. Ačkoliv se podle policejních statistik může zdát, že počtu krádeží oproti minulým letům v obchodech ubývá, realita je úplně jiná. Obchodníci mají pocit, že se spravedlnosti nedovolají, že viník buď nebude nalezen, příp. bude následně osvobozen, a tak tyto činy už prakticky nehlásí.

Dopátrat se celkového počtu krádeží je velice obtížné, odhaduje se ale, že zhruba 80 % krádeží není dále hlášeno. Takto lze odhadovat, že celkem dojde v průběhu jednoho roku v ČR zhruba k 5 400 krádežím vloupáním, v případě krádeží v obchodech se počet případů může pohybovat okolo 28 600 případů.

4.1 Modernizace kamerového systému

Jak už bylo zmíněno v předchozí kapitole, největším nedostatkem při monitorování zákazníků z hlediska bezpečnostních procesů je nízká kvalita kamerového systému využívaného v prostředí velkoobchodu. Pracovníci ostrahy se často potýkají s problémem buď zcela nefunkčního kamerového systému, popř. s nízkou kvalitou obrazu. V případě zjištění krádeží nejsou schopni za pomoci kamerového systému přesvědčivě prokázat, zda ke krádeži opravdu došlo, resp. nedošlo.

Největší překážkou při objasňování trestných činů krádeže bývá nedostatečný počet důkazů proti pachateli, resp. kvalita jejich průkaznosti. Pořízené nahrávky vydané pro účely Policie ČR bývají v tak nízké kvalitě, že pro účely následného trestního řízení jsou nepoužitelné a neprůkazné. Z dlouhodobého hlediska je trestný čin krádeže objasněn zhruba v třetině případů.

Dalším problémem, se kterým se denně obsluha kamerových systémů setkává, jsou tzv. slepá místa, tj. místa prodejní jednotky mimo kamerové pokrytí. Zde si pachatelé snaží ukrýt odcizené zboží tak, aby nebyli zaznamenáni kamerovým systémem a ostraha prodejny tak neměla žádný důkaz o zcizení zboží.

4.1.1 Kompaktní IP kamery vnitřní

Odstranění zmíněných problémů lze docílit díky modernizaci kamerového systému uvnitř prodejní jednotky, kdy navrhovaný systém disponuje dostatečně vysokou kvalitou přenosu obrazu v prostorech prodejní jednotky. Zároveň jsou obě navrhované kamery vybaveny dostatečně velkým pozorovacím úhlem pro pokrytí tzv. slepých míst.

Další výhodou navrhované modernizace kamerového systému je snazší, intuitivnější i rychlejší obsluha kamerového systému, kdy pracovníci obsluhy kamerového systému jsou schopni rychle a přesně reagovat na narušení bezpečnosti.

4.1.2 Kompaktní mini hybridní termokamera

Pro nastavení bezpečnostních procesů pro pokrytí perimetru velkoobchodní jednotky je vhodná termokamera. Její využití je přínosné pro minimalizaci škod způsobených v nočních hodinách. V konkrétním případě navrhované termokamery se obsluha kamerového systému nepotýká s problémy, které postihovaly instalované původní infrakamery. Činnost termokamery není ovlivněna počasím, čímž dochází k eliminaci falešných poplachů. Zároveň lze u konkrétní kamery nastavit rozlišení osob a zvířat.

4.1.3 Cenová kalkulace

Aby byly kamerové systémy využívané pro ostrahu prodejní jednotky užitečné nejen pro účely detekce událostí, ale také pro účely pozdější identifikace pachatelů, je nezbytné investovat do kvalitnějších kamer s vyšší kvalitou obrazu. Ačkoliv by se celkové náklady na modernizaci kamerového systému mohly zdát vysoké, musí se vzít v potaz, že pro zajištění vhodných podmínek pracovníků ostrahy při zajištění bezpečnosti velkoobchodní jednotky je třeba tuto investici akceptovat. Investice se vrátí eliminací krádeží.

Při své úvaze modernizace kamerového systému jsem zvažil jak celkové náklady, tak následnou efektivitu zabezpečení. Pracovník ostrahy nemá šanci bez kvalitního

kamerového systému střežit celý prostor velkoobchodní jednotky, dále je sníženo riziko osobního selhání zaměstnance ostrahy. Za zmínku stojí i odrazení pachatelů, resp. předpoklad snižujícího se počtu krádeží do budoucna díky kvalitnímu kamerovému systému.

4.2 Navýšení fyzické ostrahy

Pracovníci bezpečnostní agentury se momentálně potýkají s problémy spojenými s nedostatkem pracovníků ostrahy, a to jak a to jak uvnitř prodejní jednotky, tak i v prostorech parkoviště. Navýšením fyzické ostrahy dojde k odstranění problémů vyplývajících z tohoto nedostatku.

V návrhu je uvedeno navýšení o dva pracovníky bezpečnostní agentury. První na pozici strážného parkoviště, druhý na pozici detektiv prodejny. Tím lze předpokládat zvýšení efektivity zbývajících zaměstnanců ostrahy, a zároveň i zkvalitnění jejich činností.

4.2.1 Pracovník ostrahy parkoviště

Stanoviště pokladní zóny by mělo být zabezpečeno po celou otevírací dobu velkoobchodní jednotky. Strážný by tak neměl být využíván k jiným pracím, zejména na jiných stanovištích. Toho lze docílit pouze navýšením o pozici pracovníka ostrahy parkoviště.

Při zřízení této pozice dojde nejen ke zvýšení bezpečnosti v prostorech parkoviště, kdy pracovník ostrahy svou činností snižuje riziko krádeží před velkoobchodem, ale také k zajištění vyšší bezpečnosti pracovníků ostrahy při zadržování pachatele krádeže ve velkoobchodu.

4.2.2 Detektiv prodejny

Větší účinnost při odhalování krádeží v obchodech má detektiv prodejny v civilním oděvu. Nelze opomenout i preventivní opatření ostrahy prodejny ve služebním oděvu. Detektiv prodejny je ale vhodným doplněním tohoto preventivního opatření. Zároveň má pracovník ostrahy na této pozici vyšší profesní kvalifikaci, než ostatní zaměstnanci ostrahy prodejní jednotky.

Navýšením o tuto pozici dojde ke zlepšení špatných výsledků inventur způsobených krádežemi zákazníků ve velkoobchodu. V rámci zefektivnění bezpečnostních procesů u monitorování zákazníků jsem vyhodnotil navýšení této pozice za nutné. Pracovník sledující kamerové systémy může v případě zjištění krádeže dále monitorovat zákazníka pomocí kamerového systému, zároveň detektiv prodejny může provádět monitorování přímo na místě. Dojde-li k prokázání krádeže, provede zadržení pachatele, příp. pachatelů s pomocí pracovníka ostrahy.

4.2.3 Cenová kalkulace

S ohledem na nastavení bezpečnostních procesů v ostraze velkoobchodní jednotky považuji náklady spojené s navýšením fyzické ostrahy za adekvátní. Náklady na lidskou ostrahu se stále zvyšují, počtu krádeží stále přibývá.

Náklady spojené s navýšením povedou k reálnému zabránění většího počtu krádeží, díky čemuž dojde ke zvýšení efektivity z pohledu bezpečnosti. Ačkoliv má fyzická ostraha své limity, její práce je ale v prostředí velkoobchodu stále nenahraditelná.

4.3 Navýšení pevných bezpečnostních prvků

Pro úplnost nastavení bezpečnostních procesů je nezbytné dát ostraze prodejny dostatek bezpečnostních prvků. Bude-li zboží dostatečně zabezpečeno, dojde ke snížení počtu krádeží v prodejní jednotce. Zároveň bude splněna úloha prevence, kdy si zákazník jako potenciální pachatel rozmyslí svůj úmysl kradení zboží.

Nákup bezpečnostních prvků je jednorázový, naopak prvky lze využít opakovaně. Investici spojenou s navýšením bezpečnostních prvků považuji za adekvátní s ohledem na hodnotu zboží nabízeného velkoobchodní jednotkou.

Závěr

Cílem diplomové práce bylo analyzovat a profilovat podezřelé chování zákazníků v obchodě při využití poznatků z bezpečnostních procesů a technologií. Následně získané informace vhodně využít pro nastavení bezpečnostních procesů obchodu za účelem zefektivnění monitoringu podezřelých osob. Toho jsem docílil předložením návrhu na modernizaci kamerového systému, navýšení fyzické ostrahy a doplnění vhodných bezpečnostních prvků na ochranu zboží.

Diplomová práce je rozdělena do čtyř kapitol, má teoretickou, analytickou a návrhovou část, včetně zhodnocení návrhu. V teoretické části jsou využity teoretické poznatky, které jsem čerpal z odborné literatury. Záměrem teoretické části bylo umožnit čtenáři získat základní přehled týkající se bezpečnosti, typologie pachatelů krádeží a problematiky monitorování podezřelého chování v prostředí velkoobchodu. V další části je provedena analýza a identifikace problémů spojených s monitoringem. Dále je zpracován a představen návrh na efektivní zajištění ochrany osob a majetku v prostředí obchodu, včetně zhodnocení reálného přínosu návrhu. Zde jsem využil teoretické poznatky, poznatky a zkušenosti vyplývající z mé manažerské pozice u soukromé bezpečnostní agentury, dále jsem využil konzultace s odborníky, včetně vrcholového managementu vybraného subjektu z hlediska bezpečnosti.

Cena lidské práce průběžně roste, náklady na fyzickou ostrahu se zvyšují a ani rok 2022 není ve vývoji tohoto trendu výjimkou. Státem určená minimální mzda vzrostla o tisíc korun a tak se nabízí otázka, zda kamerový systém neumožní plně nahradit zastoupení fyzické ostrahy. V této základní úvaze je nezbytné zohlednit specifické potřeby v prostředí obchodu, kde je z hlediska fyzické ostrahy její místo stále nezastupitelné. Kamerový systém, včetně bezpečnostních prvků, slouží jen jako vhodné doplnění fyzické ostrahy. Na základě těchto poznatků lze konstatovat, že z hlediska logistiky bezpečnostních procesů a technologií spojených s monitoringem zákazníků nelze využít pro maximální efekt pouze některá z navrhovaných opatření, ale naopak je potřeba využít všechna navrhovaná opatření společně.

Trendy v oblasti bezpečnostního průmyslu se neustále vyvíjejí, jejich posun je viditelný v podstatě každý rok. Současně nezházejí ani pachatelé krádeží, jejichž způsoby jsou stále sofistikovanější a jejichž tvořivost prakticky nezná mezí. Vrcholové vedení

obchodu i zástupci z řad bezpečnostních manažerů musí sledovat nejnovější trendy v bezpečnostním průmyslu a ty následně vhodně využít.

V dnešní době je stále složitější rozpoznat potencionální pachatele dle kritérií negativních znaků, jelikož škála pachatelů je stále rozšířenější a vhodnou příležitostí se krádeže může dopustit téměř kterýkoliv zákazník. I z tohoto důvodu je nezbytné nastavit soubor komplexních opatření, zahrnující kombinaci fyzické i technické ochrany. To je spojeno také s výběrem vhodných zaměstnanců, kteří jsou pro výkon své činnosti dostatečně proškoleni.

Diplomová práce byla sepsána tak, aby mohla být přínosem pro vrcholový management obchodu při projednávání problematiky se zástupci soukromé bezpečnostní agentury týkající se ochrany osob a majetku, a to jak pro technické zabezpečení velkoobchodu, tak pro fyzickou ostrahu. Navrhovaná bezpečnostní opatření vychází z hodnocení současného stavu a jsou vhodná pro realizaci v aktuální době.

Seznam zdrojů

- [1] JAŠEK, Roman a David MALANÍK. *Bezpečnost informačních systémů*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013. ISBN 9788074543128. Dostupné také z: hdl.handle.net/10563/25821.
- [2] ČESKO. Zákon č. 89/2012 Sb., občanský zákoník. In: *Sbírka zákonů*. Praha: Parlament ČR, 2012, ročník 2012, částka 33/2012, číslo 89. Dostupné také z: <https://www.zakonyprolidi.cz/cs/2012-89>
- [3] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. In: *Sbírka zákonů*. Praha: Parlament ČR, 2009, ročník 2009, částka 11/2009, číslo 40. Dostupné také z: <https://www.zakonyprolidi.cz/cs/2009-40>
- [4] ČÍRTKOVÁ, Ludmila. *Forenzní psychologie*. Plzeň: Aleš Čeněk, 2004. ISBN 80-86473-86-4.
- [5] LUKÁŠ, Luděk a kol. *Bezpečnostní technologie, systémy a management*. Zlín: Radim Bačuvčík - VeRBuM, 2015. ISBN 978-80-87500-05-7.
- [6] UHLÁŘ, Jan. *Technická ochrana objektů*. Praha: Vydavatelství Policejní akademie ČR, 2005. ISBN 80-725-1189-0.
- [7] LUKÁŠ, Luděk a kol. *Bezpečnostní technologie, systémy a management*. Zlín: Radim Bačuvčík - VeRBuM, 2011. ISBN 978-80-87500-67-5.
- [8] Elektronická ochrana zboží-RF/AM/EM systémy [online]. Nučice: RAZAK SECURITY SOLUTIONS, Copyright 2022. [2022-01-23]. Dostupné z: <https://www.razak-shop.cz/elektronicka-ochrana/>
- [9] ORISshop-security systems: RF samolepící etiketa [online]. Brno: ORIS PLUS spol. s r.o. [2022-01-23]. Dostupné z: <https://www.oris-shop.cz/rf-samolepici-etiketa-4x4-bila-2-standard>
- [10] ORISshop-security systems: AM Tag s lankem [online]. Brno: ORIS PLUS spol. s r.o. [2022-01-23]. Dostupné z: <https://www.oris-shop.cz/bezpecnostni-prvek-na-ochranu-zbozi-s-integrovanym-lankem>
- [11] ORISshop-security systems: RF Capsure-Bezpečnostní plastová čepička [online]. Brno: ORIS PLUS spol. s r.o. [2022-01-23]. Dostupné z: <http://www.ochranazbozi.eu/product/detail/rf-capsure>

- [12] ORISshop-security systems: Bezpečnostní zrcadla [online]. Brno: ORIS PLUS spol. s r.o. [2022-01-23]. Dostupné z: <http://www.ochranazbozi.eu/product/default/bezpecnostni-zrcadla>
- [13] ONPIRA-Magnetický uvolňovač bezpečnostních etiket [online]. Plzeň: ONPIRA, Copyright 2022. [2022-01-24]. Dostupné z: https://www.onpira.cz/zbozi/magneticky-uvolnovac-bezpecnostnich-etiket/?gclid=Cj0KCQjwg_iTBhDrARIsAD3Ib5iauh1d71O6XGheXttVViKUoaBEd90cYbiKAEz4PIvGgn9CYNGEysMaAlgGEALw_wcB
- [14] ČESKO. Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád). In: *Sbírka zákonů*. Praha: Národní shromáždění ČSSR, 1961, ročník 1961, částka 66/1961, číslo 141. Dostupné také z: <https://www.zakonyprolidi.cz/cs/1961-141>
- [15] WALTECO: Střeženo kamerami se záznamem [online]. Uherské Hradiště, Copyright 2022 WALTECO. [2022-01-24]. Dostupné z: https://www.walteco.cz/strezeno-kamerami-se-zaznamem--cervena-297x210mm--format-a4--plastova-tabulka/?gclid=Cj0KCQjwmuITBhDoARIsAPiv6L8mqBvfjEdzI_C3jeL6dah6k8fROqm521ONbbwd1hZz6LFSnc4QBtIaAmtiEALw_wcB
- [16] Kodexy chování [online]. Praha, Copyright © 2013 Úřad pro ochranu osobních údajů. [2022-02-06]. Dostupné z: <https://www.uoou.cz/kodexy-chovani/d-29493/p1=3453>
- [17] MAKRO Cash & Carry ČR s.r.o. [online]. Olomouc: OHK, 1851-2020 © OHK Olomouc. [2022-03-05]. Dostupné z: <https://www.hkol.cz/clen/makro-cash-carry-cr-s-r-o/>
- [18] MVCR-detekce podezřelého chování [online]. Praha, © 2022 Ministerstvo vnitra České republiky. [2022-03-06]. Dostupné z: www.mvcr.cz
- [19] ALTWORX. [online]. Brno, Copyright © Altworx 2022. [2022-03-12]. Dostupné z: <https://www.altworx.com/cs/o-altworxu/#co-je-altworx>
- [20] DOUCEK, Petr a kol. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.
- [21] TSS Group. Kompaktní hybridní IP termokamera [online]. Zlín: TSS Group, Copyright © 2003–2022 TSS Group. [2022-03-27]. Dostupné z: <https://www.tssgroup.cz/dahua-tpc-bf1241-d3f4-kompaktni-hybridni-ip-termokamera>

- [22] TSS Group. IP kompaktní kamera [online]. Zlín: TSS Group, Copyright © 2003–2022 TSS Group. [2022-04-27]. Dostupné z: <https://www.tssgroup.cz/dahua-ipc-hfw5541e-ze-27135-5-mpx-kompaktni-ip-kamera>
- [23] TSS Group. PTZ IP kamera [online]. Zlín: TSS Group, Copyright © 2003–2022 TSS Group. [2022-04-27]. Dostupné z: <https://www.tssgroup.cz/dahua-sd42c212t-hn-s2-2-mpx-ptz-ip-kamera>
- [24] Luděk. Mobilizujeme. Do rukou se nám dostala rušička signálu [online]. © 2007–2022 Mobilizujeme.cz. [2022-04-27]. Dostupné z: <https://mobilizujeme.cz/clanky/dorukou-se-nam-dostala-rusicka-signalu-jak-vlastne-funguje>
- [25] Mountfield. Boční štípací kleště [online]. Strančice: Mountfield, Copyright © 2001–2022. [2022-04-27]. Dostupné z: https://www.mountfield.cz/bocni-stipaci-kleste-2dss5029?gclid=Cj0KCQjwg_iTBhDrARIsAD3Ib5gLgA3aiv3aVRSMahJ4-53f4jRVZAq2xCuA1xjOpeWBZXyrFqOhsr8aAhS5EALw_wcB
- [26] Policie ČR. Statistické přehledy kriminality za rok 2021 [online]. Praha: Policie ČR, 2022. [2022-04-27]. Dostupné z: <https://www.policie.cz/clanek/statisticke-prehledy-kriminality-za-rok-2021.aspx>

Seznam grafických objektů

Obr. 1.1 Pracovník SBS v prostoru velkoobchodu	19
Obr. 1.2 Ochranný rám	21
Obr. 1.3 Měkká etiketa	21
Obr. 1.4 Tvrdá etiketa	22
Obr. 1.5 Plastová etiketa chránící lahev alkoholu před krádeží	22
Obr. 1.6 Bezpečnostní obal	23
Obr. 1.7 Bezpečnostní prvek s integrovaným lankem	23
Obr. 1.8 Speciální bezpečnostní etiketa	23
Obr. 1.9 Bezdrátový GSM alarm	24
Obr. 1.10 Bezpečnostní zrcadlo	24
Obr. 1.11 Uvolňovač etiket	25
Obr. 1.12 Informační tabule o využití kamerového systému	30
Obr. 2.1 Schéma fází cyklu před útokem	34
Obr. 2.2 Grafické znázornění fází detekce podezřelého chování	35
Obr. 2.3 Schéma využití detekce podezřelých znaků	36
Obr. 3.1 Ilustrační obrázek IP termokamery	48
Obr. 3.2 Ilustrační obrázek vnitřní IP termokamery	49
Obr. 3.3 Ilustrační obrázek PTZ IP kamery	50
Obr. 3.4 Alobalové odstínění umístěné v kabelce	57
Obr. 3.5 Rušička radiového signálu	57
Obr. 3.6 Boční štípací kleště	58
Tab. 3.1 Základní parametry navržené IP termokamery	48
Tab. 3.2 Základní parametry navržené vnitřní IP termokamery	49
Tab. 3.3 Základní parametry navržené PTZ IP kamery	50
Tab. 3.4 Přehled navýšení pevných bezpečnostních prvků	54

Seznam zkratek

CCTV	uzavřený kamerový televizní systém – Closed Circuit TeleVision
ČR	Česká republika
DPPC	dohledové a poplachové přijímací centrum
EAS	elektronické sledování předmětů – electronic article surveillance
EPS	elektronická protipožární signalizace
EU	Evropská unie
EZS	elektronická zabezpečovací signalizace
GDPR	Obecné nařízení o ochraně osobních údajů – General Data Protection Regulation
IP	Ingress Protection
IT	informační technologie – Information technology
MP	městská policie
PC	osobní počítač – personal computer
PČR	Policie České republiky
PKB	průmysl komerční bezpečnosti
RFID	identifikace založená na rádiové frekvenci – Radio Frequency Identification
SBS	soukromá bezpečnostní služba
SMS	systém krátkých zpráv – Short message service
SPZ	státní poznávací značka

Seznam příloh

- Příloha A Cenová kalkulace modernizace kamerového systému
- Příloha B Cenová kalkulace navýšení fyzické ostrahy
- Příloha C Cenová kalkulace navýšení bezpečnostních prvků

Poznámka: Vzhledem k velikosti datových souborů příloh jsou přílohy uloženy na CD. CD je přiloženo k tištěné diplomové práci.

Autor DP	Bc. Dušan Kalup
Název DP	Logistika bezpečnostních procesů a technologií spojených s monitoringem chování zákazníků velkoobchodu
Studijní obor	Logistika
Rok obhajoby DP	2022
Počet stran	56
Počet příloh	3
Vedoucí DP	prof. Mgr. Roman Jašek, Ph.D., DBA
Anotace	Diplomová práce se zabývá problematikou logistiky bezpečnostních procesů a technologií spojených s monitoringem chování zákazníků velkoobchodu. Jsou zde objasněny pojmy jako bezpečnost, zákazník, typologie pachatelů krádeží a bezpečnostní prvky monitorování v prostředí velkoobchodu. V analytické části práce je provedena analýza současného stavu technologií a procesů pro monitorování chování zákazníků. Na základě zhodnocení analýzy je zpracován návrh na zefektivnění bezpečnostních procesů a využití bezpečnostních technologií.
Klíčová slova	bezpečnostní procesy, bezpečnostní technologie, monitoring chování osob
Místo uložení	ITC (knihovna) Vysoké školy logistiky v Přerově
Signatura	