ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

FAKULTA DOPRAVNÍ

Bc. Tatiana Tsykina

KARTOVÉ SYSTÉMY A JEJICH VLIV NA BEZPEČNOST LETIŠŤ

Diplomová práce

2019

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
Fakulta dopravní
děkan
Konviktská 20, 110 00 Praha 1

K621..... **Ústav letecké dopravy**

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

Jméno a příjmení studenta (včetně titulů):

Bc. Tatiana Tsykina

Kód studijního programu a studijní obor studenta:

N 3710 – PL – Provoz a řízení letecké dopravy

Název tématu (česky): **Kartové systémy a jejich vliv na bezpečnost letišť**

Název tématu (anglicky): ID Cards and Their Impact to Airports Security

Zásady pro vypracování

Při zpracování diplomové práce se řiďte osnovou uvedenou v následujících bodech:

- Bezpečnostní systémy letišť
- Typy karet a jejich výhody a nevýhody
- Slabá místa při identifikacích zaměstnanců na vstupu do neveřejných prostorů letišť
- Útoky hackerů a teroristů při použití informací o zaměstnancích
- Systémy pro zvýšení bezpečnosti při identifikaci osob

ČVUT FD

Rozsah grafických prací: dle pokynů vedoucího diplomové práce

Rozsah průvodní zprávy: minimálně 55 stran textu (včetně obrázků, grafů a tabulek, které jsou součástí průvodní zprávy)

Seznam odborné literatury: Koverdynský Bohdan: Letecká security: Historie, organizace, standardy a postupy, 2014.

Rankl Wolfgang, Wolfgang Effing: Smart Card Handbook 2008.

Lawrence Don: Aviation and Airport Security, 2017

Vedoucí diplomové práce: **doc. Ing. Jakub Kraus, Ph.D.**

Datum zadání diplomové práce: **27. července 2018**
(datum prvního zadání této práce, které musí být nejpozději 10 měsíců před datem prvního předpokládaného odevzdání této práce vyplývajícího ze standardní doby studia)

Datum odevzdání diplomové práce: **28. května 2019**
a) datum prvního předpokládaného odevzdání práce vyplývající ze standardní doby studia a z doporučeného časového plánu studia
b) v případě odkladu odevzdání práce následující datum odevzdání práce vyplývající z doporučeného časového plánu studia

L. S.

Kraus

doc. Ing. Jakub Kraus, Ph.D.
vedoucí
Ústavu letecké dopravy

doc. Ing. Pavel Hrubeš, Ph.D.
děkan fakulty

Potvrzuji převzetí zadání diplomové práce.

Tsykina

Bc. Tatiana Tsykina
jméno a podpis studenta

V Praze dne 27. července 2018

Poděkování

Chtěla bych poděkovat mé rodině a blízkým přátelům za pomoc a podporu během studia. Dále bych ráda poděkovala vedoucímu diplomové práce doc. Ing Jakubu Krausovi Ph.D. za odborné vedení a rady při zpracování této práce.

Prohlášení

Předkládám tímto k posouzení a obhajobě diplomovou práci, zpracovanou na závěr studia na ČVUT v Praze, Fakultě dopravní.

Prohlašuji, že jsem předloženou práci vypracovala samostatně, a že jsem uvedla veškeré použité informační zdroje v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 Zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Praze dne 28.5.2019

Tatiana Tsykina

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
Fakulta dopravní

KARTOVÉ SYSTÉMY A JEJICH VLIV NA BEZPEČNOST LETIŠŤ

diplomová práce
květen 2019
Tatiana Tsykina

ABSTRAKT

Tato práce se zabývá bezpečností letišť se speciálním zaměřením na kartové systémy, popisuje bezpečnostní legislativu a bezpečnostní modely letišť. V práci je také znázorněna problematika bezpečnostního systému letiště z pohledu vstupních prostorů pro zaměstnance, problematika identifikačních průkazů zaměstnanců letiště a možné scénáře hrozeb. Cílem této práce je znázornit nedokonalost identifikačních karet, zdůraznit problematiku při pohybu neoprávněné osoby v neveřejném prostoru letiště a navrhnout program pro optimalizaci návrhů bezpečnostních systémů letiště.

ABSTRACT

This thesis deals with airport security with special focus on card systems, it describes safety legislation and airport security models. The thesis also presents the issue of the airport security system from the employee entrance point of view, the issue of airport identification cards and possible threat scenarios. The aim of this work is to illustrate the imperfection of identification cards, to highlight the issue of unauthorized movement of people in the non-public area of the airport and to propose a program to optimize the design of airport security systems.

Klíčová slova

Bezpečnost, neveřejný prostor, letiště, ID karta, hrozba, neoprávněná osoba

Key words

Security, airside, airport, ID card, threat, unauthorized person

Obsah

Seznam použitích zkratek

ACI	Mezinárodní rada letišť	Airports Council International
AOA	Plochy k obecnému použití	Air Operations Area
ASIC	Identifikační karta letecké bezpečnosti	Aviation Security Identification Card
ATSP	Smluvní letištní bezpečnostní oblast	Airport Tenant Security Program Area
CSRA	Kritický vyhrazený bezpečnostní prostor	Critical Security Restricted Area
ČR	Česká republika	Czech Republic
ECAC	Evropská konference pro civilní letectví	European Civil Aviation Conference
EEPROM	Elektronicky Vymazatelná Paměť pouze pro čtení	Electrically Erasable Programmable Read-Only Memory
ES	Evropská společenství	European Communities
EU	Evropská unie	European Union
EUA	Vyhrazena oblast použití	Exclusive Use Area
GTD	Globální databáze terorismu	Global Terrorism Database
HiCo	Vysoká koercivita	High Coercivity
IBM	Americká mezinárodní technologická společnost	International Business Machines

ICAO	Mezinárodní organizace pro civilní letectví	International Civil Aviation Organization
ICC	Karta s integrovanými obvody	Integrated Circuit Card
ID	Identifikační karta	Identity document
ISO	Mezinárodní organizace pro normalizaci	International Organization for Standardization
IT	Informačních a komunikačních technologií	Information and Communication Technologies
LoCo	Nízká koercivita	Low Coercivit
NBP	Národní bezpečnostní program	The *national* civil aviation *security programme*
NPNV	Národní program bezpečnostního výcviku	National Security Training Program
NPŘK	Národní program řízení kvality bezpečnostních opatření k ochraně civilního	National Program for Quality Control of Security Measures for Civil Protection
NSW	Nový Jižní Wales	New South Wales
ONP	Ochrana nástupních prostorů	Protection of boarding areas
PČR	Policie České republiky	Police of the Czech Republic
PIN	Osobní identifikační číslo	Personal Identification Number

PROM	Elektricky "jednorázově" programovatelná permanentní paměť	Programmable Read Only Memory
ROM	Paměť pouze pro čtení	Read-Only Memory
SA	Zabezpečený prostor	Secured Area
SIDA	Indikační zóna bezpečnostní identifikaci	Security identification Display Area
SIM	Identifikaci účastníka v mobilní síti	Subscriber Identification Module
SRA	Vyhrazený bezpečnostní prostor	Security Restricted Area
STA	Sterilní oblast	Sterile Area
TSA	Úřad pro bezpečnost v dopravě	Transportation Security Agency
ÚCL	Úřad pro civilní letectví	Civil Aviation Authority

Úvod

Letecká doprava je neustále se rozvíjející oblastí dopravy. Je to dáno dynamickým rozvojem letišť, jakož i nárůstem pozorovaných hrozeb a neustálou potřebou zlepšit bezpečnostní postupy a zlepšit znalosti a dovednosti zaměstnanců letišť.

V letectví rozlišujeme dva druhy bezpečnosti: provozní bezpečnost (Safety) a bezpečnost, která se zabývá ochranou letectví před protiprávními činy (Security).

Vzhledem k problematice této práce se bude řešit bezpečnost z pohledu ochrany před protiprávními činy.

První část práce obsahuje základní pojmy legislativy. Dodržování legislativy je důležité pro bezpečný provoz. Zavádění bezpečnostních postupů a opatření je nejdůležitějším segmentem v provozu letišť. Security je relativně mladou částí letectví, protože předpisy, které ji regulují, vstoupily v platnost v roce 1974, kdy Mezinárodní organizace pro civilní letectví na základě terorismu a následného tlaku nastavila první standardy a vytvořila samostatnou přílohu Chicagské úmluvy číslo 17.

Po správném pochopení a dodržování legislativy, lze dodržet a navrhnout relativně bezpečný model letiště. Hlavními body pro vypracování bezpečnostního modelu jsou správné definování typu letiště, definovaní prostoru letiště a poté návrh zabezpečení letiště.

Letiště má relativně velkou plochu a slouží nejenom pro odbavení cestujících, ale také obsahuje velké množství dalších struktur, které umožňují bezpečný a rychlý provoz. Z tohoto důvodu je velice důležité správně definovat jednotlivé prostory a zabezpečit přechody mezi těmito prostory.

Jednou z důležitých věcí při zabezpečení letiště je povolení vstupu do neveřejných prostorů. Povolení lze dostat po ověření spolehlivosti. Poté může ověřená osoba požádat o identifikační průkaz letiště. Identifikační průkaz je velice důležitá část v bezpečnostním systému letiště a má velký vliv na bezpečnost. Aby se správně vybral typ karty, je potřebné zjistit výhody a nevýhody různých typů karet a správně určit typ letišť, na které to bude aplikováno. Typy karet, výhody a nevýhody jejich použití a také různé útoky pomocí identifikačních karet jsou popsány v teoretické části práce.

Po popsání celé problematiky jsou ve druhé části práce představeny tři typy scénářů, které by mohly nastat, a to při krádeži nebo ztrátě ID karty, ukončení zaměstnání a kopírování ID karty. Každý scénář popisuje nejhorší situaci, pokud by se neoprávněné osobě podařilo dostat do nejkritičtějšího prostoru. Poté je odvozován matematický model, který popisuje pravděpodobnost odhalení neoprávněně osoby mezi neveřejnými prostory.

Cílem práce je znázornit vliv identifikačních karet na celý bezpečnostní systém letiště a dokázat, že je třeba mu věnovat dostatečnou pozornost, aby byl použitelný.

V práci je dále představen systém, který by jednoduše pomocí určitých podmínek mohl navrhnout optimální rozmístění bezpečnostních zařízení pro ověření identity a bezpečnostní kontroly mezi neveřejnými prostory letiště.

1 Legislativa

Bezpečnost je nejdůležitější aspekt civilního letectví. Na bezpečnost civilního letectví se můžeme dívat ze dvou různých pohledů:

- provozní bezpečnost, která se zabývá prevencí nehod a incidentů, v angličtině je používán pojem „safety“,
- ochrana civilního letectví před protiprávními činy, kterou v ČR zajišťuje ministerstvo dopravy, v angličtině je používán pojem „security“.

Bezpečnost v letecké dopravě byla právně ustanovena už od roku 1944, předpisem úmluvy o mezinárodním civilním letectví v Chicagu. Touto úmluvou byla vytvořena Mezinárodní organizace pro civilní letectví ICAO – International Civil Aviation Organization. [1]

Legislativou v letectví se rozumí souhrn zákonů, předpisů, nařízení a doporučení, které by provozovatelé a uživatelé letiště měli dodržovat. Jedná se o doporučené minimum, při kterém by na letišti měl být zajištěn bezpečný provoz. Provozovatelé letišť mohou pravidla upřesňovat, ale nemohou snižovat požadovaná kritéria stanovená pro provoz.

Legislativu pro ochranu civilního letectví je možné rozdělit do třech skupin:

- legislativa EU,
- legislativa ČR,
- mezinárodní právní předpisy.

1.1 Legislativa EU

Během rozšiřování Evropské unie o nové členské státy nebyly stanoveny pro jednotlivé země žádné požadavky, které by musely splňovat, podmínky byly ustanoveny pouze mezi jednotlivými státy zvlášť. Z toho důvodu pak Evropská rada, v červnu roku 1993 v Kodani, určila obecné podmínky pro vstup do Evropské unie tzv. Kodaňská kritéria, která jsou souborem politických a ekonomických kritérií a obsahují také kritérium přijetí. [2]

Pro tuto práci budou stěžejní směrnice, nařízení, rozhodnutí, doporučení a stanoviska, která jsou spojena s civilní leteckou dopravou a také s bezpečnostním hlediskem v civilním letectví viz tabulka č. 1.

Tabulka 1: Legislativa EU.

Název legislativního dokumentu	Popis
Nařízení EP a Rady (ES) č. 300/2008 o společných pravidlech v oblasti ochrany civilního letectví před protiprávními činy	Stanoví základní právní rámec – společné základní normy ochrany civilního letectví před protiprávními činy na úrovni Evropské unie. [3]

Nařízení Komise (EU) č. 1254/2009.	Toto nařízení stanoví kritéria umožňující členským státům odchýlit se od společných základních norem v oblasti ochrany civilního letectví před protiprávními činy a přijmout alternativní bezpečnostní opatření. [3]
Nařízení Komise (EU) 2015/1998	Provádí opatření ke společným základním normám ochrany civilního letectví před protiprávními činy a nastavení bezpečnostních opatření pro subjekty. [3]
Nařízení komise (EU) č. 185/2010, kterým se stanoví prováděcí opatření ke společným základním normám letecké bezpečnosti	Velice důležitý dokument, obsahuje již celkem podrobné požadavky a vymezení (definice). Rozpracovány společné základní normy z ES č. 300/2008.
Rozhodnutí Komise (EU) K (2015) 8005	Rozhodnutí upřesňující postupy provádění jednotlivých bezpečnostních opatření a charakterizující podmínky udělení výjimek. Na národní úrovni aplikováno prostřednictvím § 86d leteckého zákona (základní opatření). [3]
Nařízení komise (ES) č. 272/2009, kterým se stanoví prováděcí opatření ke společným základním normám letecké bezpečnosti	Stanovuje obecná opatření doplňující společné základní normy stanovené v příloze nařízení (ES) č. 300/2008. Například udává povolené metody detekční kontroly. [4]
Doporučení Evropské konference pro civilní letectví ECAC Doc No. 30, Part II - Security	Tento dokument se zaměřuje na zajištění bezpečnostních opatření na ochranu civilního letectví před protiprávními činy. Zahrnuje bezpečnostní ustanovení na úrovni členských států a letišť. [4]

1.2 Legislativa ČR

Hlavním leteckým zákonem v České republice je **Zákon č. 49/1997 Sb.** – Zákon o civilním letectví, což je zákon regulující civilní letectví v ČR.

Osmá část tohoto zákona **č**. 49/1997 Sb. přímo odkazuje na ochranu civilního letectví před protiprávními činy, zahrnuje v sobě sedm hlav:

I. Hlava první. OBECNÁ USTANOVENÍ O OCHRANĚ CIVILNÍHO LETECTVÍ PŘED PROTIPRÁVNÍMI ČINY
II. Hlava druhá. SPOLEHLIVOST
III. Hlava třetí. OCHRANA LETIŠŤ, LETADEL, CESTUJÍCÍCH A ZAVAZADEL
IV. Hlava čtvrtá. OCHRANA NÁKLADU, POŠTOVNÍCH ZÁSILEK A VĚCÍ LETECKÉHO DOPRAVCE
V. Hlava pátá. ODBORNÉ POŽADAVKY
VI. Hlava šestá. PROSTŘEDKY SLOUŽÍCÍ K OCHRANĚ CIVILNÍHO LETECTVÍ PŘED PROTIPRÁVNÍMI ČINY
VII. Hlava sedmá. ZÁKLADNÍ, ZVLÁŠTNÍ A MIMOŘÁDNÁ OPATŘENÍ [5]

Z pohledu bezpečnosti letecké dopravy také jsou důležité vyhlášky viz tabulka č. 2:

Tabulka 2: Vyhlášky.

Název	Popis
Vyhláška MDS č. 108/1997 Sb.	Prováděcí vyhláška zákona o civilním letectví.
Vyhláška MDS č. 222/2000 Sb.	Vyhláška o nerovnoměrném rozvržení pracovní doby některých zaměstnanců v civilním letectví.
Vyhláška MD č. 410/2006 Sb.	Vyhláška o ochraně civilního letectví před protiprávními činy a o změně vyhlášky č. 108/1997.
Vyhláška MD č. 466/2006 Sb.	O bezpečnostní letové normě, ve znění vyhlášky č. 60/2009 Sb. [4]

Z pohledu zákona jsou dále důležité tyto zákony:

- Zákon č. 262/2006 Sb., Zákoník práce. Upravuje právní vztahy mezi zaměstnancem a zaměstnavatelem. Upravuje práva a povinnosti zaměstnanců a zaměstnavatelů.
- Zákon č. 361/2003 Sb., zákon o služebním poměru příslušníků o bezpečnostních sborů. Jedná se o zákon, který stanovuje podmínky práce osobám, které vykonávají svou práci v bezpečnostním sboru. Bezpečnostním sborem se rozumí Policie České republiky, Hasičský záchranný sbor České republiky, Celní správa České republiky, Vězeňská služba České republiky, Generální inspekce bezpečnostních sborů, Bezpečnostní informační služba a Úřad pro zahraniční styky a informace.

- Zákon č. 101/2000 Sb., Zákon o ochraně osobních údajů a o změně některých zákonů. Zákon přímo není spojený s bezpečnostním programem, ale při návrhu realizace je nutné respektovat ochranu osobních údajů. [3]

1.3 Mezinárodní právní předpisy

Mezinárodní právní předpisy jsou souhrn různých zákonů, nařízení a vyhlášek, které musí členské státy dodržovat. Hlavní organizaci v letecké dopravě, která se zabývá koordinací, organizací a zajištěním bezpečného provozu civilní letecké dopravy je Mezinárodni organizace pro civilní letectví.

1.3.1 L 17 - ICAO Annex 17

Jak již bylo uvedeno v kapitole č. 1, legislativa se začala zavádět po Chicagské úmluvě (Úmluva o mezinárodním civilním letectví), která byla podepsaná v roce 1944. Hlavní, co bylo zavedeno při podepsání Chicagské úmluvy, je Mezinárodni organizace pro civilní letectví (ICAO).

Mezinárodni organizace pro civilní letectví přejímá normy pro civilní letectví ve všech oblastech. [3]

Z tohoto důvodu ICAO vypracovala několik leteckých předpisů, kterými se musí členské státy řídit, pokud zároveň podepsali Úmluvu o mezinárodním civilním letectví.

V současnosti je ustanoveno 19 hlavních leteckých předpisů (Annexů), a to konkrétně:

L1 – ZPŮSOBILOST LETECKÉHO PERSONÁLU CIVILNÍHO LETECTVÍ

L2 – PRAVIDLA LÉTÁNÍ

L3 – METEOROLOGIE

L4 – LETECKÉ MAPY

L5 – POUŽÍVÁNÍ MĚŘICÍCH JEDNOTEK V LETOVÉM A POZEMNÍM PROVOZU

L6 – PROVOZ LETADEL

L7 – POZNÁVACÍ ZNAČKY LETADEL

L8 – LETOVÁ ZPŮSOBILOST LETADEL

L9 – ZJEDNODUŠENÍ FORMALIT

L10 – LETECKÁ TELEKOMUNIKAČNÍ SLUŽBA V CIVILNÍM LETECTVÍ

L11 – LETOVÉ PROVOZNÍ SLUŽBY

L12 – PÁTRÁNÍ A ZÁCHRANA V CIVILNÍM LETECTVÍ

L13 – ODBORNÉ ZJIŠŤOVÁNÍ PŘÍČIN LETECKÝCH NEHOD A INCIDENTŮ

L14 – LETIŠTĚ

L15 – LETECKÁ INFORMAČNÍ SLUŽBA

L16 – OCHRANA ŽIVOTNÍHO PROSTŘEDÍ

L17 – BEZPEČNOST, OCHRANA MEZINÁRODNÍHO CIVILNÍHO LETECTVÍPŘED PROTIPRÁVNÍMI ČINY

L18 – BEZPEČNÁ LETECKÁ DOPRAVA NEBEZPEČNÉHO ZBOŽÍ

L19 – ŘÍZENÍ BEZPEČNOSTI

Vzhledem k tomu, že se práce zabývá problematikou bezpečnostního systému letišť, ze všech leteckých předpisů bude stěžejní předpis L 17 „Bezpečnost, ochrana mezinárodního civilního letectví před protiprávními činy“, plnohodnotným předpisem stal až v roce 1974. [1]

Jedná se o jeden z hlavních dokumentů, kterým se řídí provozovatelé letišť pro modelování bezpečnostního systému pro dané letiště. [6]

Hlavní podmínkou, kterou musí splnit provozovatel letiště podle předpisu L 17 je vypracování a zavedení Národního bezpečnostního programu (dále jenom NBP) ochrany civilního letectví před protiprávními činy. Předpis L 17 vyžaduje, aby členské státy určily příslušný úřad pro vydávání, aktualizaci, kontrolu a koordinaci zavádění NBP.

NBP můžeme dále rozdělit na Národní bezpečnostní program ochrany civilního letectví České republiky před protiprávními činy, Národní program bezpečnostního výcviku v civilním letectví České republiky a Národní program řízení kvality bezpečnostních opatření k ochraně civilního letectví ČR před protiprávními činy viz obrázek č. 1

Obrázek 1: Národní bezpečnostní programy

- Národní bezpečnostní program ochrany civilního letectví České republiky před protiprávními činy.

NBP je hlavním dokumentem pro ochranu civilního letectví a jeho cílem je zabránit událostem, které mohou mít dopad na bezpečnost civilní letecké dopravy.

Ministerstvo dopravy má na starost vytváření systému pro ochranu civilního letectví před protiprávními činy a také koordinaci bezpečnostních opatření k ochraně civilního letectví před protiprávními činy. Úřad pro civilní letectví (ÚCL) má za úkol zavádění a kontrolu

bezpečnosti, vytváří NBP a kontroluje zavedení tohoto systému. Velice úzce spolupracuje s ministerstvem dopravy při zavádění bezpečnostních postupů a opatření. NBP je nejdůležitější dokument pro tvorbu a modelování bezpečnostního systému letiště. V tabulce č 3. jsou uvedeny v části NBP. [7]

Tabulka 3: Obsah NBP programu.

NBP	
Část	**Popis**
Část I	Definice pojmů
Část II	Cíl a hlavní zásady NBP
Část III	Vydání, koordinace a kontrola zavádění NBP
Část IV	Vnitrostátní právní předpisy, právní předpisy Evropských společenství a mezinárodní právní předpisy, z nichž NBP vychází
Část V	Ochrana informací
Část VI	Rozpis činností a odpovědnosti. Státní správa na úseku ochrany civilního letectví před protiprávními činy
Část VII	Bezpečnostní program letiště, bezpečnostní program leteckého dopravce, bezpečnostní program poskytovatele letových provozních služeb, bezpečnostní program subjektu uplatňujícího normy ochrany letectví před protiprávními činy
Část VIII	Mezirezortní komise pro bezpečnost civilního letectví a Letištní výbor pro bezpečnost
Část IX	Bezpečnostní opatření a postupy
Část X	Vyhodnocování účinnosti bezpečnostních opatření, šetření případů ohrožení bezpečnosti civilního letectví
Část XI	Informace o ohrožení bezpečnosti civilního letectví, vyhodnocení hrozeb a šetření protiprávních činů
Část XII	Mimořádná opatření a postupy v situacích s konkrétní hrozbou
Část XIII	Mimořádné bezpečnostní situace za letu
Část XIV	Krizové situace
Část XV	Mezinárodní spolupráce

- Národní program bezpečnostního výcviku v civilním letectví České republiky

Jeden z programů, který reguluje NBP je NPNV, což je národní program, který má za cíl zajistit vhodný způsob přijímání a školení pracovníků všech právnických a fyzických osob pracujících v civilním letectví. Hlavním úkolem NPNV je, aby všichni pracovníci civilního letectví

absolvovali takové bezpečnostní školení, které by jim umožnilo vykonávat svou práci na odpovídající úrovni. [8]

- Národní program řízení kvality bezpečnostních opatření k ochraně civilního letectví ČR před protiprávními činy

NPŘK má za úkol zavádění účinné a efektivní kontroly bezpečnostních opatření pro provozovatele letišť, letecké dopravce, poskytovatele letových provozních služeb a pro subjekty, které uplatňují normy pro ochranu letectví před protiprávními činy.

NPŘK je systém, který má dvě úrovně organizační struktury:

1. První stupeň tvoří úřad.

Úřad je odpovědný za kontrolu zavedení NPŘK, tedy vydávání průkazů a vedení auditorů, vyhodnocování efektivity a kvality bezpečnostních opatření a postupu na národní úrovni ze zjištěných dat.

2. Druhým stupněm je vnitřní systém kontrolování kvality.

Provozovatelé letišť, letečtí dopravci, poskytovatelé letových provozních služeb a další subjekty, které uplatňují normy pro ochranu letectví před protiprávními činy, jsou odpovědni za vytvoření a zavedení vnitřního systému řízení kvality. Zároveň jsou odpovědni za provedení kontroly a dodržení bezpečnostních postupů a opatření, vyhodnocování nedostatků a odborný výcvik svých zaměstnanců.

Společným cílem těchto dvou úrovní je tedy vyhodnocení a odstranění nedostatků pro kvalitní fungování. [9]

1.3.2 Montrealský protokol.

V roce 1988 byl podepsán protokol o boji s protiprávními činy a násilí na letištích sloužících k mezinárodnímu civilnímu letectví. Protokol doplňuje Úmluvu o potlačování protiprávních činu ohrožujících bezpečnost civilního letectví z roku 1971. Montrealská úmluva byla podepsaná v roce 1971 v Montrealu.

Montrealský protokol doplňuje montrealskou úmluvu tak, že rozšiřuje působnost ustanovení na teroristické činy, které byly spáchány na mezinárodních civilních letištích. Protokol se také týká násilných a protiprávních činů proti osobám na mezinárodních letištích, proti letištním zařízením nebo letadlům na zemi. [1]

2 Základní rozdělení letištních prostorů

Letištěm rozumíme vymezenou plochu na zemi nebo vodě, která je určena pro vzlety, přistání a pojíždění letadel. Obvykle k letištní ploše patří i technické a logistické stavby: hangáry, letištní terminály, sklady a letecké stavby.

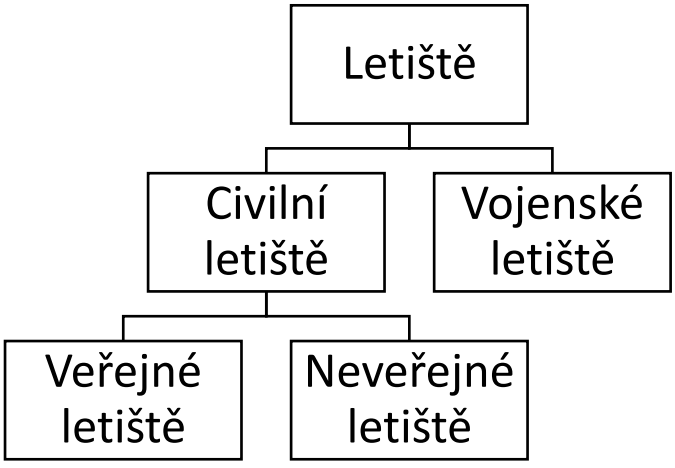
Vzhledem k tomu, že letiště jsou využívána pro různé účely, není přesně stanoveno konkrétní rozdělení. Druhy letišť se dají určit podle různých hledisek:

- podle okruhu uživatelů,
- podle provozních podmínek a základního určení,
- podle rozsahu poskytovaných letových služeb,
- podle druhu provozu,
- podle typu přiblížení podle přístrojů,
- podle obchodního provozu,
- podle počtu cestujících,
- podle úlohy.

Hlavní rozdělení letišť, která nás budou zajímat, jsou dělení podle okruhu uživatelů, dělení podle provozu a dělení podle počtu cestujících. [10]

2.1 Rozdělení letišť podle okruhu uživatelů

Rozdělením letiště podle okruhu uživatelů rozumíme, zda je letiště určeno pro civilní leteckou dopravu nebo slouží vojenským účelům.



Obrázek 2: Základní rozdělení letišť

Civilní letiště můžeme ještě rozdělit na dvě kategorie a to na veřejné a neveřejné letiště (viz obrázek č. 2).

- Veřejným letištěm se rozumí letiště, na kterém je povoleno provozovat všechna civilní letadla a všechny civilní lety, přičemž jediná podmínka, která musí být splněna, je technické vybavení letiště, které musí odpovídat bezpečnému provozu určitého typu letadla.

- Neveřejné letiště je civilním letištěm, ale na tomto typu letiště lze vykonávat lety osobami s povolením. Před použitím neveřejného letiště musí uživatel dostat od provozovatele letiště souhlas k povolení k provozu, tj. povolení pro vzlet a přistání.
- Vojenské letiště je letiště, které je určeno pro provoz ozbrojených sil a jiných podobných státních struktur. [10]

2.2 Rozdělení letišť podle typu provozu

Letiště podle typu provozu můžeme rozdělit do dvou kategorií:

- Vnitrostátní letiště – je letiště, které slouží pro provoz letů uvnitř určitého státu. To znamená, že lety nepřekračují hranice státu.
- Mezinárodní letiště – je letiště, které je určeno jen pro provoz letů, při kterých dochází k překročení státní hranice. [10]

2.3 Rozdělení letišť podle počtu cestujících

V rámci Evropy můžeme všechna veřejné letiště podle Mezinárodni rady letišť (ACI - Airports Council International) rozdělit do čtyř skupin dle závislosti na počtu odbavených.

- I – do první skupiny patří letiště, která za rok odbavila více než 25 milionů pasažérů.
- II – druhá skupina zahrnuje letiště, která odbavila 10 až 25 milionu pasažérů za rok.
- III – do třetí skupiny patří letiště, která odbavila 5 až 10 milionu pasažérů za rok.
- IV – čtvrtá skupina letišť je skupina, zahrnující odbavení méně než 5 milionů pasažérů za rok. [10]

Rozdělení podle okruhu uživatelů, typu provozu a počtu odbavených cestujících, která byla popsána výše, je důležité pro plánování bezpečnostního systému. Základ pro bezpečnostní systém bude na všech letištích stejný, odlišují se pak jednotlivá rozdělení letišť.

V této práci budou řešena letiště sloužící pro civilní účely. Podle NBP programu není přesně stanoveno rozdělení letištních prostorů, které musí letiště dodržovat. Pro modelování bezpečnostního systému letiště je nutné, aby provozovatel letiště podal vytvořený bezpečnostní program na schválení ÚCL. Teprve po jeho schválení se může začít s budováním bezpečnostního systému.

Prostory letiště můžeme logicky rozdělit na fyzické prostory, radiové prostory, IT prostory a perimetr letiště.

2.4 Fyzické prostory

Fyzické prostory můžeme rozdělit na dvě části podle účelů využití a podle bezpečnostního systému:

2.4.1 Letištní prostor

Letištní prostor (Airside) je vyhrazený prostor, na kterém dochází k omezenému pohybu. Tato část v sobě zahrnuje části letiště za bezpečnostní kontrolou, které jsou dostupné pro cestující

a zaměstnance, přičemž zaměstnanci pro vstup do neveřejného prostoru potřebují identifikační karty. [4]

Neveřejný prostor letiště spadá pod letištní prostor. Do neveřejného prostoru patří všechny stavby nebo součásti staveb, k nimž je potřeba kontrolovat přístup. K neveřejné části letiště zároveň patří přilehlý terén letiště a také pohybové a odbavovací plochy.

Z pohledu zaměstnance letiště je to jakýkoliv prostor, do kterého je potřeba mít ke vstupu identifikační průkaz, ale neprovádí se při něm bezpečnostní kontrola. [4]

2.4.1.1 Neveřejný prostor se zvláštním režimovým opatřením

Neveřejný prostor se zvláštním režimovým opatřením je určitý vyhrazený prostor v neveřejné části letiště. Vytváří se v některých případech podle potřeby provozovatele letiště. Vstup do toto prostoru je umožněn za stejných podmínek, jaké jsou u vstupu do SRA prostoru. [4]

2.4.1.2 SRA prostor

SRA prostor je část neveřejného prostoru letiště, který je určen provozovatelem letiště. Vstup do tohoto prostoru je kontrolován pro zajištění ochrany civilního letectví před protiprávními činy.

SRA prostor v sobě zahrnuje: všechny prostory pro cestující mezi detekční kontrolou a nástupem do letadla, odbavovací plošiny, prostor pro třídění zavazadel, sklady a prostory pro přípravu cateringu. [4]

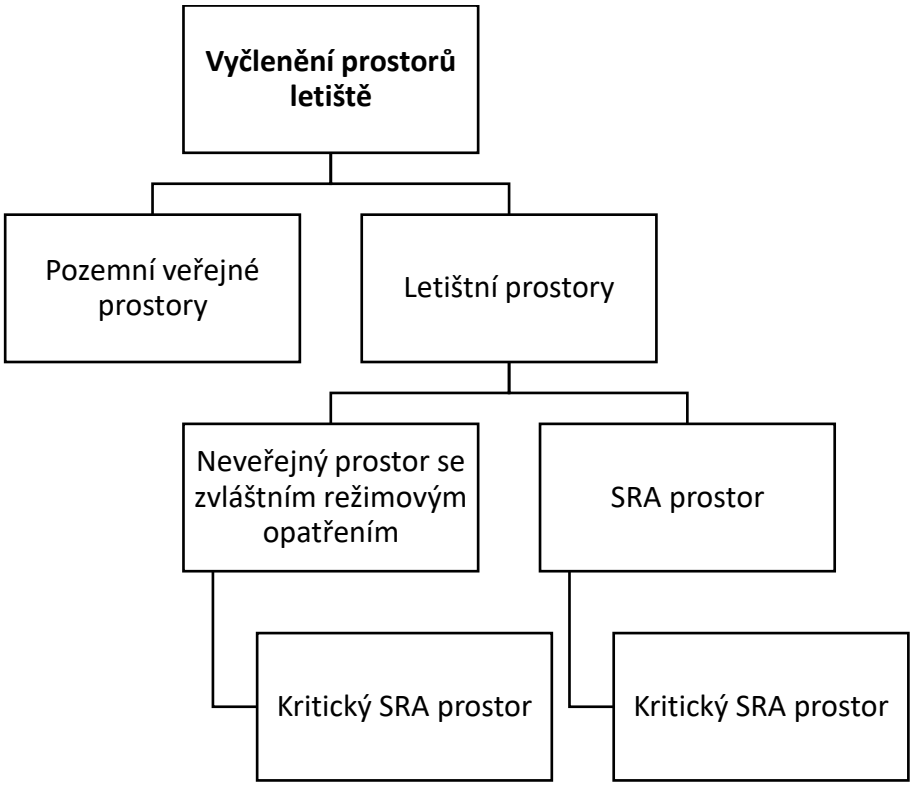
2.4.1.3 Kritický SRA (CSRA)

Dle definice se kritický SRA prostor nachází mezi bezpečnostní kontrolou a nástupem do letadla. [4]

2.4.2 Pozemní veřejné prostory

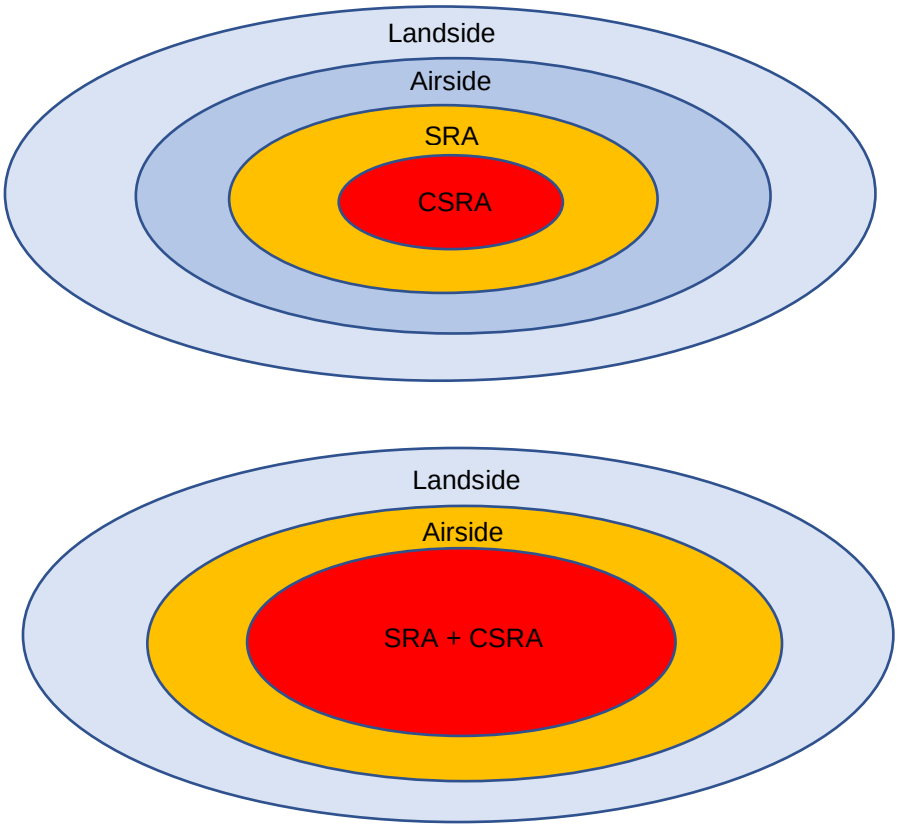
Pozemní veřejné prostory (Landside) jsou vyhrazené prostory, které jsou určené k volnému pohybu. Většinou zahrnují venkovní prostor před terminály, parkoviště, příletové a odletové haly, odbavovací přepážky, čekací prostory apod.

Civilní dopravní letiště používají rozdělení svých prostorů podle možnosti přístupu: veřejný prostor, neveřejný prostor, neveřejný prostor se zvláštním režimovým opatřením, SRA (Security Restricted Area) prostor a kritický SRA prostor. SRA prostor a neveřejný prostor se zvláštním režimovým opatřením je podmnožinou neveřejných letištních prostorů i kritický SRA prostor je podmnožinou SRA prostoru a neveřejného prostorou se zvláštním režimovým opatřením viz obrázek č. 3. [4]



Obrázek 3: Vyčlenění prostorů

Z provozního hlediska většinou letiště využívají dva typy rozdělení viz obrázek č. 4, kde prostor SRA je sloučeny nebo odděleny s prostorem kritická SRA. V praxi se většinou můžeme potkat na letišti se sjednoceným SRA prostorem a kritickým SRA prostorem.



Obrázek 4: Základní rozdělní letištních prostorů.

3 Struktura a popis modelování bezpečnostního systému

Základní úlohy pro modelování bezpečnostního systému letiště jsou:

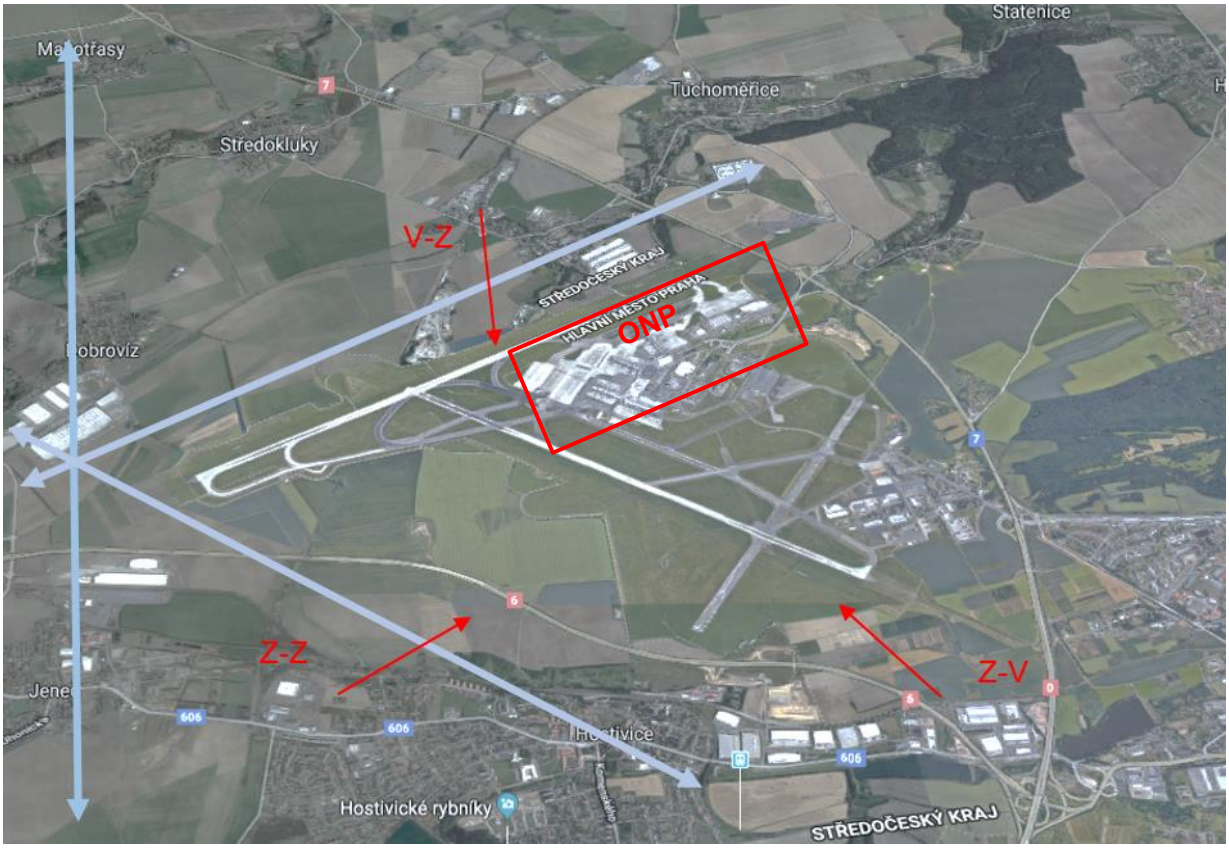
- detekovat narušitele nebo hrozbu,
- vyhodnotit sílu hrozby nebo rizika.

3.1 Typy narušení

Typy narušení můžeme rozdělit na několik typů: narušení perimetru, narušení uvnitř perimetru a ostatní narušení (elektromagnetická narušení, IT – kybernetická narušení).

3.1.1 Narušení perimetru

Aby bylo možné naplánovat bezpečnostní systém, musíme nejdříve vyhodnotit všechny možné směry ochrany.



Obrázek 5: Směry ochrany.

Na obrázku č. 5 jsou na příkladu pražského letiště znázorněny možné směry ochrany a možné směry hrozby.

- <u>země – země</u>

U směru ochrany z-z se jedná o porušení pozemního perimetru. Zároveň se jedná o ochranu perimetru.

- vzduch – země

Porušení typu v-z se označuje jako porušení pozemního perimetru ze vzduchu. Proto je v tomto případě důležitá definice vzdušného perimetru a určení zařízení, které by mohlo detektovat narušení vzdušného perimetru.

- země – vzduch

Třetí směr ochrany může nastat v případě možného ohrožení dopravního prostředku ze země.

3.1.2 Narušení uvnitř perimetru

Narušení uvnitř perimetru je velice obsáhlý pojem. Jedná se o narušení, které může proběhnout uvnitř perimetru a zároveň to je narušení, které je nejdůležitější z pohledu této práce. Je to neoprávněný vstup nebo pokus o vstup neoprávněné osoby do neveřejných prostorů, kterými se zabýváme. Na obrázku č. 5 je znázorněna oblast, kde se jedná o ochranu nástupních prostorů (ONP).

V kapitole č. 2.4 bylo již znázorněno základní dělení letištních prostorů, ale z pohledu celého perimetru, můžeme letištní perimetr rozdělit na oblasti, viz obrázek č. 6:

- Plochy k obecnému použití (AOA - Air Operations Area)

Oblasti letiště, kde se pohybují letadla.

- Smluvní letištní bezpečnostní oblast (ATSP - Airport Tenant Security Program Area)

Prostor, ve kterém se mohou pohybovat zaměstnanci cizích firem, které mají smlouvy s letištěm.

- Vyhrazena oblast použití (EUA -Exclusive Use Area)

Prostor, ve kterém převzal zodpovědnost za bezpečnost jiný subjekt, např. letecký dopravce.

- Zabezpečený prostor (SA - Secured Area)

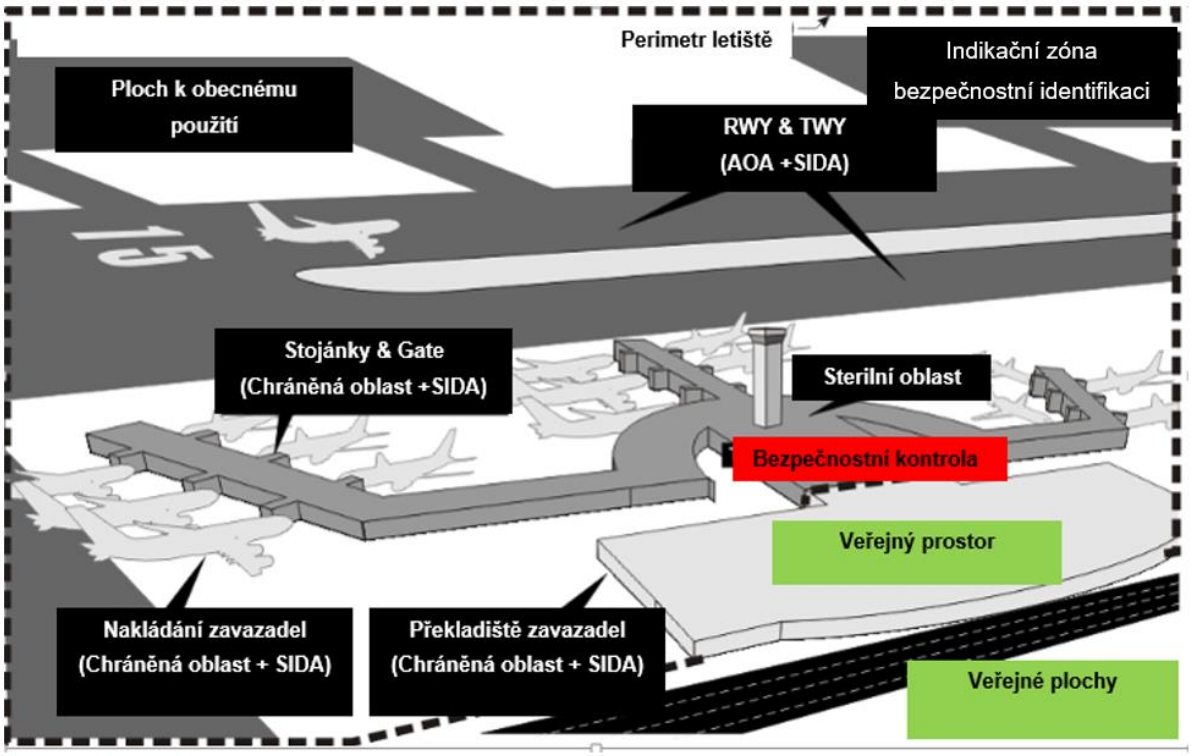
Oblast, ve které jsou dodržovány zvláštní bezpečnostní předpisy, např. prostor, ve kterém se vykládají zavazadla

- Indikační zóna bezpečnostní identifikaci (SIDA - Security identification Display Area)

Všechny oblasti, ve kterých je požadováno dodržování bezpečnostních opatření, např. SA nebo ATSP.

- Sterilní oblast (STA - Sterile Area)

Oblast přístupu cestujících k letadlům, obecně oblast mezi bezpečnostní kontrolou a nástupním prostorem. [11]



Obrázek 6: Rozdělení ploch uvnitř perimetru. [11]

3.1.3 Ostatní typy narušení

- elektromagnetické narušení – jedná se o narušení provozu, kterým může být například uměle vytvořený výpadek rádia, radaru apod.
- IT – (kybernetická narušení) – napadení hackery řídicí IT systémy na letišti.

3.2 Model bezpečnostního systému

Jak je výše uvedeno v kapitole kapitoly č. 1.3.1. (L 17 - ICAO Annex 17), musí podle leteckého předpisu L17 musí každý provozovatel letiště vypracovat bezpečnostní program. Přesná osnova a struktura bezpečnostního programu je popsána v NBP.

Obsah bezpečnostního programu provozovatele letiště má 7 kapitol:

I. Základní ustanovení
II. Popis letiště
III. Bezpečnostní opatření na letišti
IV. Nábor a odborná příprava pracovníků
V. Vnitřní kontrola kvality
VI. Pohotovostní plánovaní
VII. Přílohy

Tento obsah musí každý provozovatel letiště vyplnit tak, aby splňoval podmínky pro bezpečný provoz letiště. [4]

3.2.1 Základní procesy pro tvorbu bezpečnostního programu letišť

Pro vytvoření správného bezpečnostního systému letiště tak, aby splňoval všechny podmínky NBP a stanovený obsah bezpečnostního programu, existuje proces tvorby bezpečnostního systému.

1. První, z čeho se skládá tvorba bezpečnostního procesů, je sběr informací o zabezpečení na letiště. Níže jsou uvedeny základní informace, které by měl provozovatel letiště mít:
    - majetkové vztahy na letišti,
    - zónování letiště,
    - definice typů prostorů,
    - definice typů uživatelů,
    - případy využití letiště
    - vyhodnocení nezbytného zabezpečení
2. Dále, by měl provozovatel letiště vytvořit pohotovostní plán proti protiprávním činům.
3. Pokračovaní ve sběru informací ohledně bezpečnosti.
4. Posledním bodem je vypracování bezpečnostního systému. [4]

3.3 Zabezpečení letiště

Zabezpečením letiště se rozumí místa, která potřebují dodržování určité úrovně bezpečnosti. Nejdůležitějším krokem je definování míst, procesů a bezpečnostních prvků, které by zajišťovaly bezpečnostní proces.

Také je důležité pro zabezpečení letiště definovat osoby, které se pohybují mezi prostory letiště. Tyto osoby budeme dále definovat jako aktéry.

3.3.1 Základní rozdělení pohybujících se osob na letišti

Aktéry na letišti jsou fyzické osoby, které jsou přímo závislé na systému zabezpečení letiště. Proto je nutné definovat všechny typy aktérů pro vytváření bezpečnostního systému letiště. Jejich definování je jedním ze základních procesů pro tvorbu bezpečnostního systému viz kapitola č. 3.2.1.

Na letišti se můžeme setkat s několika druhy aktérů. Vzhledem k problematice diplomové práce, můžeme rozdělit aktéry do třech skupin. První skupinu tvoří aktéři, kteří pro vstup do neveřejné části letiště nepotřebují ID kartu. Těmito aktéry jsou:

- Cestující – jsou jedním z nejdůležitějších typů aktérů na letišti, ovšem tento typ aktérů nesouvisí s problematikou této práce.

Další skupinou pohybujících se aktérů na letišti jsou osoby, které mají dlouhodobě identifikační kartu. Těmito aktéry jsou:

- zaměstnanci letiště – dlouhodobě identifikované osoby, které mají omezený pohyb mezi prostory letiště v závislosti na místu výkonu zaměstnaní,

- speciální typy zaměstnanců – ke speciálním typům zaměstnanců patří osoby, které mají vystaveny dlouhodobě firemní ID karty, většinou to jsou zaměstnanci dozorových orgánů.
- PČR a CP – Police České republiky a Celní police jsou také držiteli dlouhodobých ID karet a jsou zvláštním druhem aktérů, kteří mají výjimky v bezpečnostních pravidlech. [12] [4]

Třetí skupinou jsou aktéři, které mají pro vstup do veřejných prostorů letiště jednorázové ID karty. Vstup pomocí jednorázové ID karty můžeme rozdělit do dvou kategorií. První kategorií je vstup do prostorů, kde není vyžadován doprovod a druhá kategorie prostorů, je vstup, kde vyžadován doprovod.

Prostory, do kterých je vyžadován doprovod, jsou SRA zóna, neveřejný prostor se zvláštním režimovým opatřením a kritický SRA prostor. Doprovod může vykonat osoba, která už je držitelem trvalé a platné ID karty letiště.

Aktéry využívajícími jednorázové karty jsou:

- zaměstnanci externích subjektů – typ aktérů, který se objevuje na letišti nepravidelně. Mohou jimi být například zaměstnanci stavebních firem.
- dodavatelé – aktéři, kteří poskytují zásobování letiště.
- návštěvy – druh aktérů, který také pro vstup potřebuje jednorázovou ID kartu. Návštěvy musí být obvykle nahlášeny předem a pro vyřízení jednorázové ID karty by se návštěvníci měli prokázat platným dokladem totožnosti. [13] [4]

Z kapitoly č. 3.2.1 už je známo, že při plánování bezpečnostního systému letiště, je jedním z prvních požadavků zónování letiště, neboli rozdělení letiště na jednotlivé prostory podle provozu a potřebné úrovně bezpečnosti.

V kapitole č. 2.4 je představeno základní rozdělení jednotlivých prostorů. Při přechodu mezi těmito prostory je potřebné aplikovat zařízení pro dodržování potřebné úrovně bezpečnosti.

3.3.2 Bezpečnostní prvky

V celém prostoru letiště se musí dodržovat určitá úroveň bezpečnosti, a zároveň je nutné udržovat jednoduchost zařízení na jednotlivých přechodech a určit správný poměr mezi cenou a výkonem.

Prvky bezpečnostního systému můžeme rozdělit na:

1. Aktivní
    - Bezpečnostní prvky
    - Ostatní prvky
2. Pasivní

Za aktivní bezpečnostní prvky můžeme považovat prvky, které mají aktivní integraci s aktéry. Účelem takových prvků je zajišťovat bezpečnost. Aktivní prvky jsou:

a. Kamerový systém
b. Bezpečnostní pracovníci
c. Pasová kontrola s pracovníkem
d. Pasová kontrola automatická
e. Rámové detektory kovů
f. Rentgenový skener příručních zavazadel
g. Ruční skener kovů
h. Osobní prohlídka
i. Skenery kapalin
j. Další moderní bezpečnostní zařízení pro odhalení nebezpečných předmětů
k. Bezpečnostní skenery a detektory zapsaných zavazadel
l. Kontrola nedoprovázených zavazadel, nákladu a pošty
m. Čtečky karet
n. Automatické dveře
o. Turnikety
p. Závory, brány, pásy s hřeby pro proražení pneumatik
q. Perimetrické radary
r. Detektory pohybu

Mezi ostatní aktivní prvky bezpečnostního systému patří jakékoliv prvky, které se aktivně integrují s aktéry, a jejich účelem není přímo zajišťování bezpečnosti letecké dopravy. To jsou například: [4]

a. Turnikety umožňující průchod při pomocí ID karty
b. Detektory kouře a nebezpečných látek

Mezi pasivní prvky letištního bezpečnostního systému patří všechny prvky, které se nachází na letišti a které je možné využít pro bezpečnost letiště. K pasivním prvkům patří:

a. Struktura budovy terminálu
c. Ploty
d. Přenosné zábrany
e. Struktura odbavovací plochy, SRA

Vzhledem k tomu, že se zabýváme se problematikou ID karet a vlivem na bezpečnostní systém letišť, nás budou zajímat aktivní bezpečnostní prvky.

ID karty v praxi můžeme využívat spolu se mnohými systémy, proto je nejdřív lepší pochopit funkčnost a technologii samotných karet. [4]

4 Typy karet a jejich charakteristiky

Plastové karty dnes hrají důležitou roli v našem životě, jelikož je využíváme každý den. Karty používáme pro různé účely – placení, ověření identity, vstupy pomocí karty, klubové karty atd. Plastové karty jsou velice populární a užitečný nástroj, protože mají vhodnou velikost, vyšší životnost (než jiný druh karet).

Zavádění prvních karet bylo zahájeno ve Spojených Státech Amerických. První karty nebyly vyrobené z plastu, ale z papíru. V roce 1914 velké americké banky začaly vydávat stálým klientům, kteří měli jejich důvěru, kreditní karty. V roce 1928 firma „Farrington Manufacturing“ v Bostonu začala vyrábět metalické karty s reliéfním vytlačením jména a adresy. To umožnilo prodavači pomocí kopírovacího papíru rychle okopírovat údaje klientů. Důsledkem zavedení tohoto systému, byl značný nárůst počtu klientů.

V roce 1960 firma IBM (IBM - International Business Machines) po domluvě s vládou Spojených Států vyvinula technologii pro bezpečné chránění informací na plastových kartách.

V současné době se můžeme setkat s různými typy plastových karet:

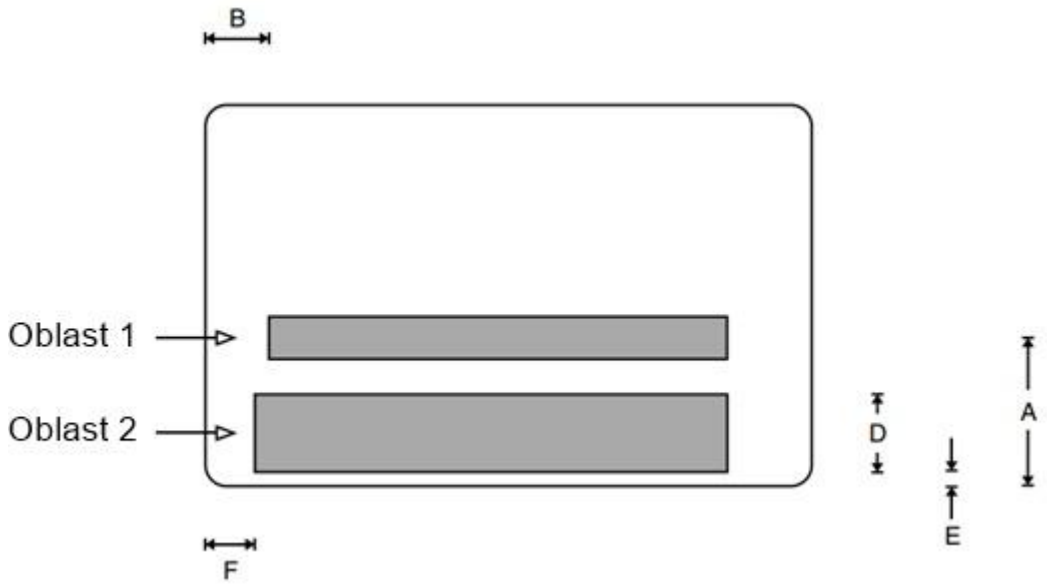
- Reliéfní karty.
- Magnetické karty.
- Smart karty. [14]

4.1 Reliéfní karty

U reliéfních karet je využíván nejstarší způsob kontroly identity. Symboly, které jsou vytlačeny na kartě mohou, být přeneseny na papír při použití jednoduchých a levných přístrojů. Také lze velice jednoduše přečíst symboly, které jsou na kartě vytlačené, což je pro jednoduchost kontrol dostačující.

Aby bylo možné vytvořit přístroj, který by jednoduše kontroloval (kopíroval údaje z karty), rozhodlo se o zavedení jednotného systému pro všechny výrobce plastových reliéfních karet. Hlavním požadavkem od výrobce bylo umístění vytlačených symbolů.

Dále byl zaveden standart ISO 7811 „Identification Cards – Recording Technique“, který je v současné době rozdělen na pět částí a popisuje nejenom reliéfní karty, ale také karty s magnetickým proužkem a čipové karty. [15]



Obrázek 7: Rozmístění vytlačených symbolů na reliéfní kartě. [15]

První část standartu popisuje požadavky na vytlačené znaky, včetně tvaru, velikosti a výšky znaků.

Druhá část definuje přesné umístění znaku na kartě a definuje dvě oddělené oblasti. Oblasti karty jsou znázorněny na obrázku 7.

První oblast je určená pro identifikační číslo karty, které identifikuje vydavatele karty i držitele karty. Obvykle má toto číslo 16 znaků. Druhá oblast je vyhrazena pro další údaje týkající se držitele karty, jako je jeho jméno a adresa.

Rozestupy mezi 1. a oblastí 2. jsou vidět na obrázku č. 7, rozestupy jsou označeny jako A až F (A = 21.42 ± 0.12 mm, B = 10.18 ± 0.25 mm, D = 14.53 mm, E = 2.41−3.30 mm, F = 7.65 ± 0.25 mm). [15]

4.1.1 Výhody a nevýhody reliéfních karet

Hlavní výhoda přenosu informaci tiskem je jednoduchost techniky - a skutečnost, že při této technologii není potřeba připojení k elektrické ani telefonní síti.

Základní nevýhodou reliéfních karet je to, že jejich použití vytváří hodně papíru, který je drahý na zpracování. [16]

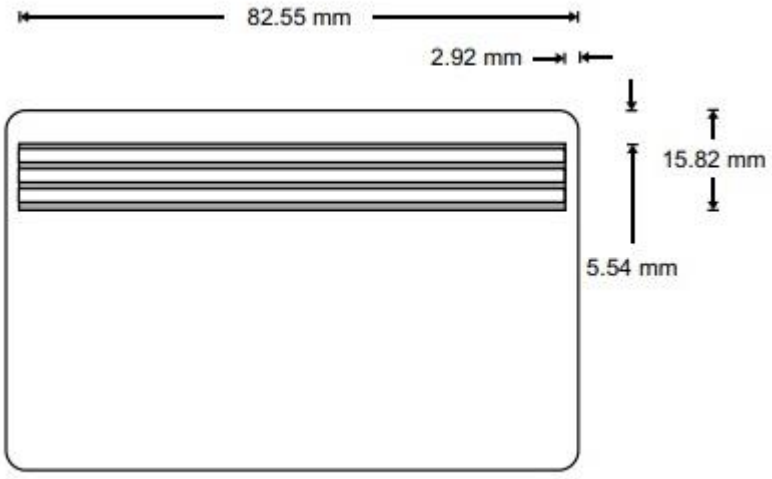
4.2 Magnetické karty

V kapitole č. 4.1.1 jsou popsány nevýhody používaní reliéfních karet. Vzhledem k narůstající popularitou reliéfních karet a přibývajícím množstvím uživatelů se však práce s tímto typem karet začala značně komplikovat. Z tohoto důvodu se začalo přemýšlet nad systémem, který by mohl ulehčit práci s plastovými kartami a zároveň zvýšit bezpečnost při zpracování.

Jedním z řešení bylo digitální kódování údajů na kartě pomocí magnetického proužku, který je umístěný na zadní straně karty.

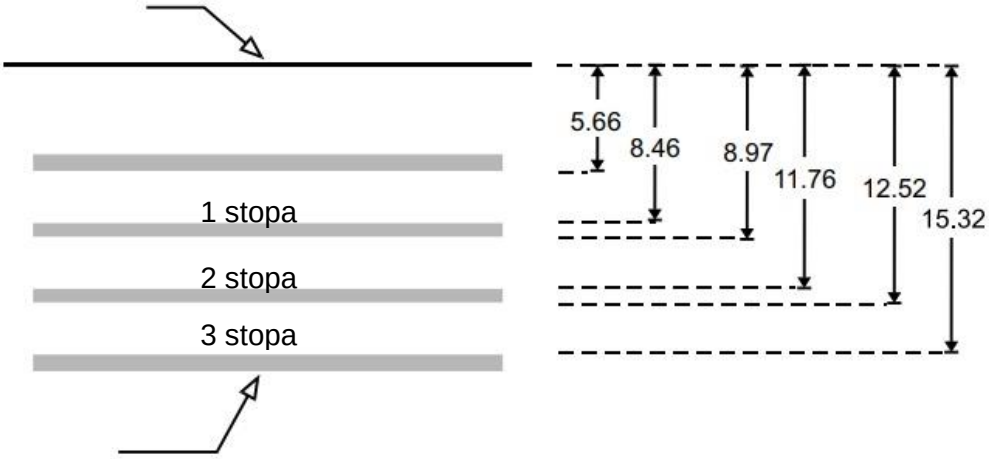
Magnetický proužek může být přečten speciálním přístrojem, který umí přečíst elektronická data, která jsou na něm zakódovaná.

Části 2., 4. a 5. normy ISO 7811 specifikuji vlastnosti magnetického proužku, techniku kódovaní a umístění magnetického proužku viz obrázek č. 8. [15]



Obrázek 8: Rozmístění magnetického proužku na plastové kartě. [15]

Magnetický proužek v sobě může mít tři drážky viz obrázek č. 9. První a druhá drážka je určená pouze pro čtení, třetí drážka je používaná pro zapisování kódů.



Obrázek 9: Rozmístěni magnetických stop. [15]

V tabulce č. 4, jsou popsány technické charakteristiky drážek – maximální množství znaků a počet symbolů, které mohou být použity. Na magnetický pasek je možné zapsat až 1000 bitů, což není příliš, ale stačí to pro chránění základních informací. Popřípadě mohou být doplňující údaje nahrány na třetí drážku.

Tabulka 4: Technické charakteristiky magnetických drážek. [15]

Drážka	Počet symbolu	Symboly kódovaní
1. Drážka	Maximálně 76	QWERTYUIOPASDFGHJKLZXCVBNM 1234567890 : ; = + ( ) – ‘ - ! @ # ^ & * <> / \
2. Drážka	Maximálně 37	Jenom čísla: 1234567890 a znak "="
3. Drážka	Maximálně 104	Jenom čísla: 1234567890 a znak "="

Magnetický pásek může být vytvořen pro různou sílu magnetického pole a podle tohoto parametru je možné rozdělit karty na dva druhy podle typu magnetického proužku:

- vysoko koercitivní (HiCo),
- nízko koercitivní (LoCo).

Stupeň koercivity ovlivňuje kvalitu stability zaznamenaných informací vůči demagnetizaci. Plastové karty s magnetickém proužkem HiCo jsou více spolehlivé. [15]

4.2.1 Výhody a nevýhody karet s magnetickém proužkem

Karty s magnetickém proužkem mají několik výhod:

- magnetické karty mají kompaktní velikost, což je velice příjemné pro uživatele,
- v této kompaktní velikosti obsahují magnetické karty velké množství informací a magnetický proužek může obsahovat základní informace karty (číslo karty, platnost karty) jméno držitele karty a PIN - kód karty (PIN – Osobní identifikační číslo).
- výroba karet s magnetickým proužkem je relativně levná, proto jde o nejběžnější typ karet.

Hlavní nevýhoda technologie s magnetickým páskem je to, že informace může být velice snadno změněna. Například u reliéfních karet je těžší změnit původní informace a hlavně změna karty bude zjevná. Změna na kartách, které mají magnetický pásek, může být provedena při standartním čtením informace nebo zapisování nové informace a následně je velice těžké dokázat změnu informací.

Další velkou nevýhodou karet s magnetickým proužkem je nedostatečná síla nosiče (magnetická páska podléhá mechanickým a jiným účinkům) a taky nemožnost aktualizovat data, protože požadavek na údržbu karty je dostupný jen v režimu připojení k síti.

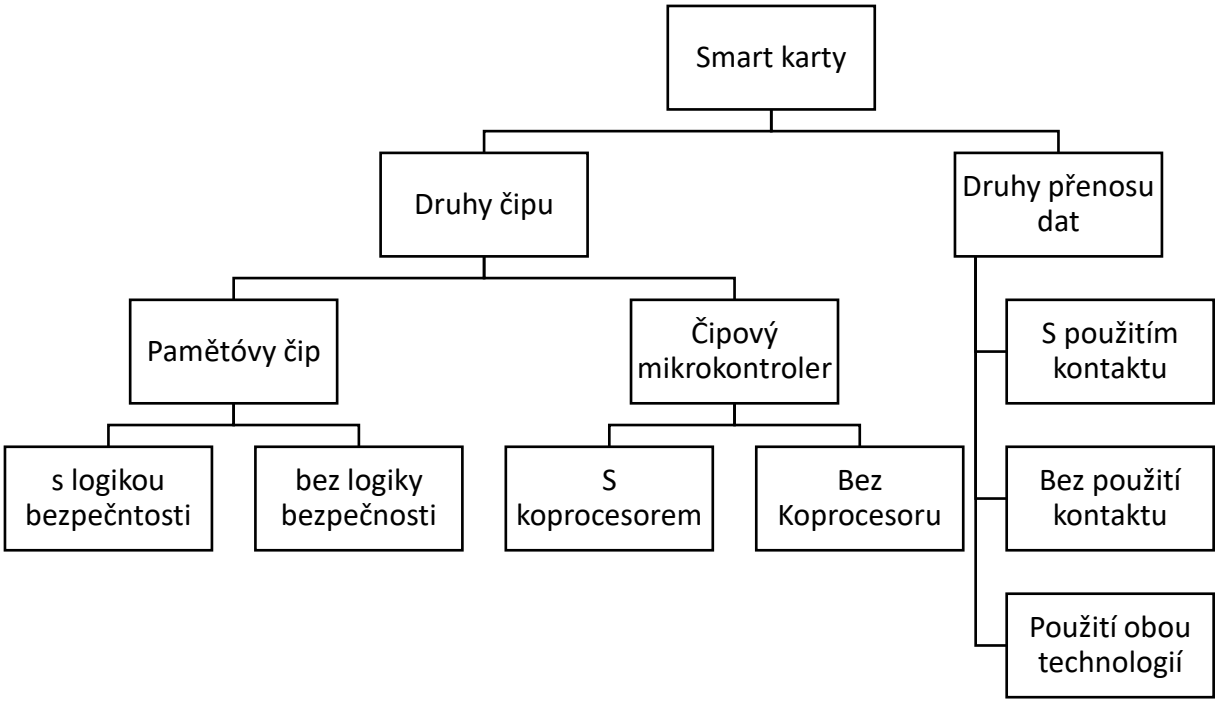
Kromě toho jsou karty s magnetickým proužkem často využívány v automatických přístrojích, ve kterých vizuální kontrolování není možné (např. bankomaty). Potenciální zloděj, který má údaje karty, může snadno zhotovit kopii, bez potřeby kopírovat vzhledové funkce bezpečnosti. Výrobci karet s magnetickým proužkem rozpracovali různé způsoby ochrany údajů proti kopírování. [16]

4.3 Smart karty

Vzhledem k tomu, že karty s magnetickým proužkem mají nevýhody (popsány výše v kapitole č. 4.2.1), se dá říct, že plastové karty s magnetickým proužkem nejsou vhodné pro využití v procesech, vyžadujících vetší míru zabezpečení.

V současné se už většinou setkáváme s plastovými kartami typu „Smart karty“.

Smart karty nebo také čipové karty jsou nejnovějším druhem karet. Hlavním specifikem je integrální schéma, které je zabudované do karty. Schéma v sobě obsahuje komponenty pro předání, chránění a zpracování údajů. Údaje mohou být předávány nebo za použití elektromagnetického pole – tzv. bezkontaktní karty viz obrázek č. 10. [17]

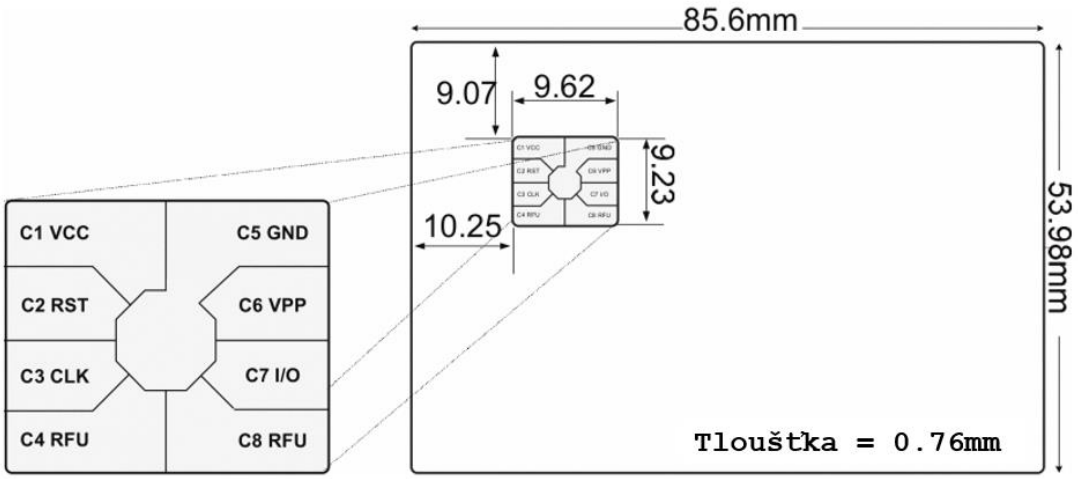


Obrázek 10: Druhy Smart karet.

4.4 Fyzické a elektrické vlastnosti

Smart karta je plastová karta, která má stejnou velikost, jako standartní platební karta se zabudovaným mikročipem. Smart karta je více bezpečná a může chránit více informací než karta s magnetickým proužkem. Smart karta má ICC (z angličtiny integrated circuit card), což je mikrokontrolér s vnitřní pamětí. Informace může být uchovaná v paměti a jsou vytvořeny systémy zabezpečující informace.

Fyzické rozměry smart karty jsou popsány v normě ISO 7810. Rozměry karty jsou 85,6 mm X 53.98 mm, a úhlový rádius je 3,18mm, a s tloušťkou 0.76mm. O rozmístění mikro schématu bylo rozhodnuto v roce 1988 a je popsáno v normě ISO7816-2 viz obrázek č. 11. [15]

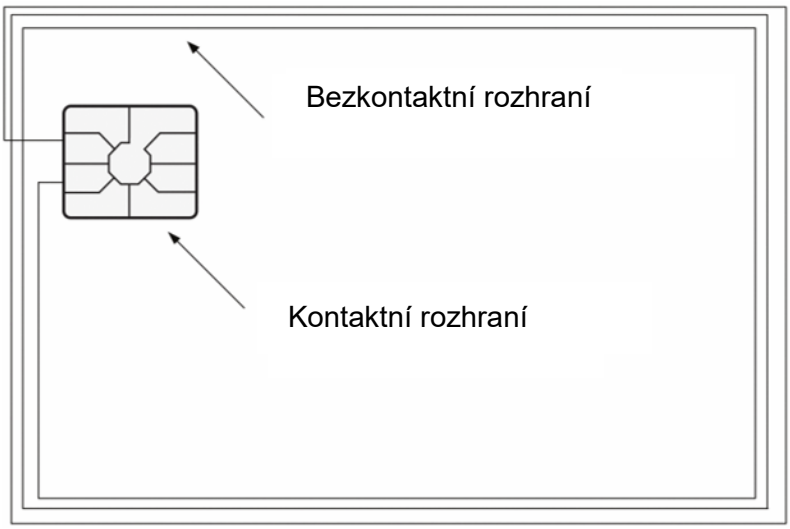


Obrázek 11: Rozmístěni čipu na Smart kartě. [15]

Karta může být použita kontaktně nebo bezkontaktně s využitím elektromagnetického rozhraní. Podle způsobu využití (kontaktní či bezkontaktní) můžeme rozdělit smart karty na dvě kategorie – kontaktní smart karty (ISO 7816) a bezkontaktní smart karty (ISO 1443, typ B). V současné době existují karty s dvěma rozhraními viz obrázek č. 12.

Kontaktní karty mají čip, který má 8 kontaktů, a jak je ukázáno na obrázku č 11, každý z těchto kontaktů plní určitou funkci.

Bezkontaktní karty mají zabudovaný čip s mikroprocesorem, který v sobě má radiový přijímač a anténu. Bezkontaktní spojení funguje pouze při velmi blízké vzdálenosti se čtečkou. Technologie smart karty s bezkontaktním spojením je dražší, ale praktičtější.



Obrázek 12: Rozmístění rozhraní. [15].

4.5 Typy Smart karet

Existuje několik typů klasifikace Smart karet, například typ s mikroschématem, který je zabudovaný v kartě. Nebo také podle typu funkcí, které smart karta má. Nejjednodušší karty mají v sobě pouze paměť, složitější v sobě mají počítač, který zvládá velké množství operací.

4.5.1 Typy mikroschémat

Do karty mohou být zabudovány tyto druhy schémat:

- karty s permanentním programovatelným přístrojem pro zapamatování (PROM – anglicky Programmable Read Only Memory). Jedná se o nejjednodušší typ karet, jejíž hlavní využití je v telekomunikaci (SIM karty),
- karty s přeprogramovatelnou pamětí, které jsou závislé na energii (EEPROM – Electrically Erasable Programmable Read-Only Memory) umožňují přepisovat informace. Hlavní využití – uložení osobních údajů,
- karty s nepřeprogramovatelnou pamětí, které umožňují číst nebo zapsat informace při použití speciálního kódu. Využívají se jako platební karty, nebo jako karty k ochraně osobních údajů.
- mnohofunkční karty mají v sobě velký objem energie (EEPROM) závislý na paměti a také speciální mikroprocesor, který má mikrooperační systém. Tyto karty se dají použít pro jakékoliv potřeby. [15]

4.5.2 Využiti karet

- Karty – počitadla – jsou využívány pro takový typ počítání, kdy je potřeba odčítat určité množství od celkové sumy. Takové karty jsou nejvíce ve světě využívány pro telefonní paměťové karty. Majitel může uskutečnit určité množství telefonních hovorů, protože

v telefonních automatech má jednotka času určitou cenu. Karta funguje jenom v kontaktním režimu.

Při každém kontaktu na kartě jsou odčítány bity z paměti karty. Po vyčerpání bitů karta přestává fungovat. Analogický způsob je používaný při placení za dopravu, parkování apod. [15]

- Paměťové karty jsou využívány pro chránění informací. Z názvu je zřejmé, že mikro schéma má v sobě pouze přístroj pro zapamatování informací. Existují dva typy těchto karet – se zabezpečenou a nezabezpečenou pamětí.
- Karty s mikroprocesorem – fungují podobně jako paměťové karty, ale mikro schémata v sobě mají mikroprocesor.

  Mikroprocesor je mikro schéma (čip), které je schopno zachovat velké množství dat a které je schopné dělat matematické a logické operace.

  Mikro procesor je instalován do smart karet a má následující charakteristiky:
  - frekvence je 5 MHz,
  - operační paměť do 256 bit (pro vyplňování příkazu),
  - ROM (z anglického Read-Only Memory) do 10 kbit (pro chránění operačního systému) [15]

Tyto karty splňují velké množství úloh. Jedná se o speciální možnost blokování pro nelegální použití karty. Karty mohou být použity jenom při zadání správného kódu, Karta bude zablokovaná při zadání nesprávného kódu. Většinou má uživatel tři pokusy pro zadání správného kódu.

4.5.3 Výhody a nevýhody čipových karet

Smart karty mají několik výhod o proti kartám s magnetickým páskem.

Například:

- maximální objem paměti je několikanásobně větší. V současné době existuji čipové karty, které v sobě mají více než 256 kB. Objem paměti je vetší s každou novou generací mikroschémat.
- Hlavní výhodou Smart karet je to, že uložené údaje na kartě mohou být zabezpečeny proti neoprávněnému přístupu a manipulaci. Je to z důvodu šifrování dat na kartě, ke kterým se dá dostat pouze přes speciální operační systém, určený pro tento typ karet.

V zásadě lze omezit hardwarové i softwarové mechanismy, pro omezení mohou být použity ukládání, mazání a čtení dat a jejich propojení s konkrétními podmínkami. To umožňuje vytvořit řadu bezpečnostních mechanismů, které mohou také být přizpůsobeny specifickým požadavkům konkrétní aplikace. V kombinaci se schopností vypočtu kryptografických algoritmů a

neustálou přítomnosti karet u uživatelů, je možné u čipových karet implementovat velké množství bezpečnostních modulů.

Dalšími výhodami čipových karet jsou jejich vysoká spolehlivost a dlouhá životnost. Např. ve srovnání s magnetickými proužky, jejichž životnost je obvykle omezena na jeden nebo dva roky.

Bezkontaktní karty mají několik výhod:

- Mohou být využity v jednu chvíli několika uživateli.
- Při využití bezkontaktního spojení se zmenšuje opotřebování karty.

Integrální schémata smart karet mají značný progres ve sféře identifikace a značně zvyšují bezpečnost soukromých údajů. [15] [17]

4.6 ID karty

ID – je z angličtiny „Identity Dokument“. ID karta je oficiální doklad prokazující totožnost, včetně elektronických systémů různých úrovní a účelů a obvykle ve formátu plastové karty.

Identifikační karta obvykle obsahuje informace o držiteli karty v textu, strojově čitelném a elektronickém formuláři, včetně jeho fotografie, jména, osobního čísla, podpisového vzoru, data platnosti, biometrických informací zaznamenaných na elektronickém čipu nebo na magnetickém proužku. V ideálním případě bude obsahovat maximální množství informací nezbytných pro bezpečné fungování. [18]

V předchozích kapitolách jsme se zabývali tím, jaké typy karet existují a jaké mají výhody a nevýhody. Vzhledem k problematice této práce, se dále budeme zabývat jen potenciálními problémy a událostmi, které mohou nastat u ID karet.

4.6.1 Teroristické útoky

Dnes je koncepce bezpečnosti dopravy primárně vykládána jako varování před terorismem v dopravě. Protiteroristický imperativ bezpečnosti dopravy je objektivní povahy a je obecně způsoben výrazným nárůstem teroristických činů ve světě, jakož i mírou jeho nebezpečí přímo v dopravně. [1]

Letečtí dopravci a provozovatelé letišť musí neustále zdokonalovat bezpečnostní opatření. Ovšem jak ukazuje historie, nová bezpečnostní opatření byla vždy provedená až po spáchání teroristického činu.

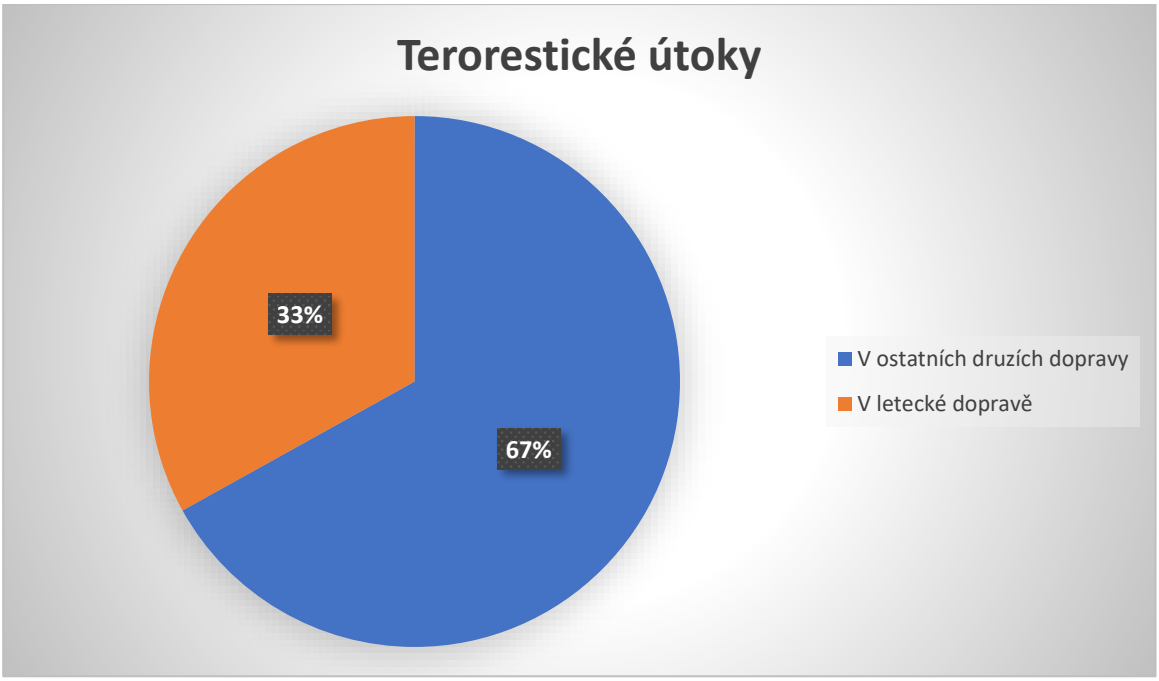


Diagram 1: Teroristické útoky v dopravě za posledních 20 let.

Globální databáze terorizmu (GTD - Global Terrorism Database), kterou aktualizuje univerzita v Marylandu. Databáze obsahuje informace o teroristických událostech po celém světě od roku 1970 až do roku 2017 (s dalšími ročními aktualizacemi plánovanými do budoucna).
Po vyhledávání spáchání činu v konkrétním období a v konkrétním odvětví, lze jednoduše určit poměr mezi spáchanými teroristickými činy v dopravě celkem a letecké dopravě zvlášť.
Z diagramu č. 1 je vidět, že ze 100 procent spáchaných teroristických činu v dopravě je 33 procent pravě v letecké dopravě. [19]
V letecké dopravě se stalo hodně různých teroristických útoků, ale nejhorším útokem v historii se stalo 11. září v roce 2001. Poté ve Spojených státech Amerických byl vytvořen Úřad pro bezpečnost v dopravě (TSA – Transportation Security Agency), který definoval letištní prostory a určil podmínky pro vstup aktérů do těchto prostorů. TSA požaduje po všech letištích, které spadají pod Federální leteckou správu, aby zaváděli letištní bezpečnostní plány a definovali letištní prostory. [1]
Dále také došlo k vytvoření nových bezpečnostních postupů, takových jako:

- zabránění vstupu nepovolaným osobám do vnitřního prostoru letiště,
- důsledná kontrola cestujících, posádek letadel a jejich zavazadel,
- důsledná kontrola nákladu, zboží, pošty a ostatních přepravovaných věcí,
- konstrukce letadel s ohledem na zabránění vniknutí do pilotní kabiny,
- přítomnost ozbrojené ostrahy na palubách rizikových letů

4.6.2 Útoky s využitím ID karty zaměstnance

Pod pojmem útoky s využitím ID karet zaměstnanců můžeme rozumět kopírování ID karty zaměstnanců nebo krádež ID karet.

V jednom z případů můžeme brát kopírování a krádež jako stejnou událost, protože ve výsledku se jedná o útok, který byl spáchán na celý bezpečnostní systém letiště a v obou případech se jedná o krádež osobních údajů.

Ve druhém případě můžeme kopírování chápat jako nezávislý útok na celý bezpečnostní systém letiště. To znamená, že kopírování jedné konkrétní karty či více karet, se dá říct, že útok nebyl pomocí celého bezpečnostního systému, ale pomocí vnější části - ID karty.

Krádež ID karty můžeme brát ze dvou různých pohledu. Prvním je fyzická krádež a druhým je krádež osobních údajů přes kyberprostor.

Kyberprostor může také sloužit jako platforma pro provádění teroristických útoků proti leteckému průmyslu. Kromě odborné debaty o možnosti způsobit skutečné škody při kybernetickém útoku na letišti a na letadla, je třeba řešit i několik nedostatků v této oblasti. V historii letecké dopravy bylo několik útoků spojených s útoky hackerů na bezpečnostní systém letiště.

Jeden z posledních útoků byl v červenci 2018 na společnost, která vydává průkazy totožnosti pro leteckou bezpečnost. Byl to útok hackerů, což vedlo k obavám, že v důsledku toho by mohla být bezpečnost letišť ohrožena. A to proto, že průkazy totožnosti jsou určeny k tomu, aby zabránily zločincům nebo teroristům v přístupu k letadlům a jiným omezeným letištním zónám. Stovky lidí, kteří se ucházejí o Identifikační karty letecké bezpečnosti (ASIC - Aviation Security Identification Card) nebo jej obnovují prostřednictvím společnosti NSW Aviation ID Australia, obdrželi e-maily, ve kterých jim sdělili, že jejich informace o aplikacích ASIC mohou být odcizeny.

Je také potřeba zmínit důležitost identifikace ne jenom na letištích s velkým provozem, ale i s malým provozem. Identifikace osob je opravdu důležitou součásti bezpečného provozu. Jeden z příkladů zavádění ID karet je případ, který se stal na letišti Letňany v Praze. V tomto případě se nejedná o zneužití ID karty, při kterém byl spáchán čin, ale o zavádění ID karet po spáchání činu. [20]

V srpnu 2015 na letišti Praha Letňany byl spáchán útok, při kterém došlo k vniknutí neoprávněné osoby do prostoru letiště (do hangáru) a následně došlo k vážnému poškození letadla. Poté, aby letiště mohlo dodržovat platný letištní řád a bylo schopno eliminovat možná rizika v souladu s Národním bezpečnostním programem zavedlo 15 července 2015 systém ověření identity na letišti Letňany a systém ID karet.

Jeden z požadavků systému ID karet bylo rozdělení letištního prostoru na jednotlivé bezpečnostní zóny. Bezpečnostní systém taktéž vyžaduje, aby všechny osoby pohybující se na území letiště Letňany nosili ID kartu na viditelném místě. [21]

5 Vyhodnocení aktuálních problémů

Předchozí kapitoly (viz kapitola č. 4) se zabývaly historií, technickými funkcemi, problematikou ID karet, také legislativou, leteckými předpisy a bezpečnostním systémem letišť.

V této kapitole je cílem znázorněnou problematiku systému spojeným s ID kartami viz kapitola 4.6, vyhodnotit a určit místa, kde by mohlo dojit ke selhání systému (selhání systému – pokus, neoprávněné použití nebo neoprávněný pokus o vstup, vjezd)

V teoretické části této práce, přesně z kapitol č. 2 a 3 se dá říct, že identita osoby (zaměstnance letiště) je jedna z nejdůležitějších věcí, kterou musí provozovatel letiště zajistit podle leteckých předpisů L17 – Bezpečnostní ochrana mezinárodního civilního letectví před protiprávními činy, hlava č. 4 – preventivní bezpečnostní opatření, kapitola č. 2 opatření vztahující se ke kontrole vstupu a vjezdu.

V kapitole č. 4 ohledně funkčních nedokonalostí různých typu karet, problematiky systému a taky jaké jsou nevýhody v použití.

Praxe dokazuje, že v současné době existují mnohem spolehlivější systémy pro identifikaci osoby za pomocí biometrických údajů, jako je například otisk prstu, geometrie obličeje nebo rohovka oka. Analýzu problematiky budeme provádět pro letištní bezpečnostní systém. V této kapitole budeme zabývat konkrétními problematickými případy a místy, kde by mohlo dojít k selhání systému.

Z kapitoly č. 2.4 už víme jedno logické rozdělení letištního prostoru. Je to rozdělení na veřejnou a neveřejnou část. Neveřejnou část můžeme rozčlenit na několik úrovní, například podle úrovně potřebného bezpečnostního opatření: neveřejný prostor, neveřejný prostor se zvláštním režimovým opatřením, SRA prostor a kritický SRA prostor.

Dle kapitoly č. 4.6 ohledně teroristických činů a útoku hackerů, které byly spáchané v letectví, bylo vytvořeno tři scénáře:

1. Krádež nebo ztráta ID karty.
2. Ukončení zaměstnání.
3. Kopírovaní ID karty.

Tyto tři scénáře ukazují na problematiku (možné chyby) v bezpečnostním systému letišť. Každý scénář je rozdělený na části podle typu přestupu mezi jednotlivými prostory letišť.

První část scénáře je přechod mezi veřejným a neveřejným prostorem. Jedná se o jednoduchý přechod mezi dvěma prostory, většinou pro průchod mezi těmi prostory není vyžadováno velké opatření, obvykle pro přestup mezi veřejnou a neveřejnou části je potřeba jen ID karta zaměstnance a jednoduchý turniket.

Druhá část scénáře je přechod mezi neveřejným prostorem letiště a SRA prostorem nebo neveřejným prostorem se zvláštním režimovým opatřením. Na tomto typu přestupu obvykle kontrola se provádí pomocí kovového detektoru, rentgenu a taky osobní prohlídky.

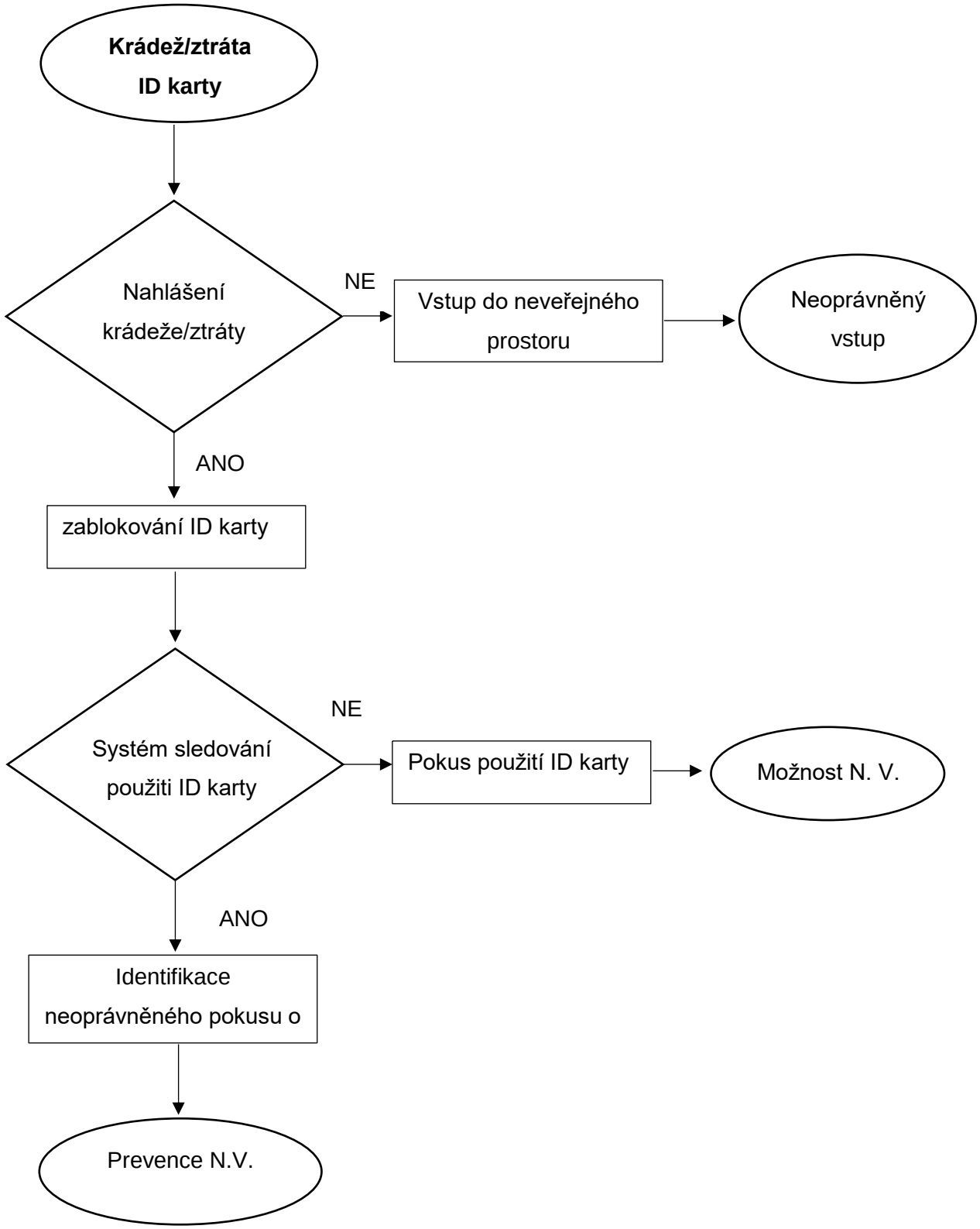
Třetí část scénářů je přechod mezi SRA prostorem nebo neveřejným prostorem se zvláštním režimovým opatřením a kritickým SRA prostorem. Z kapitoly č. 2.4 je známo, že letiště může určit rozdělení svých prostorů. Kritická SRA je prostor, na kterém provozovatel letiště může požadovat zvýšené podmínky bezpečnostních opatření.

5.1.1 Krádež nebo ztráta ID karty

První scénář zahrnuje dvě velice podobné problematiky, a to krádež ID karty a ztrátu ID karty. Shodnost problematik je v tom, že při ztrátě i krádeži může dojít ke zneužití ID karty.

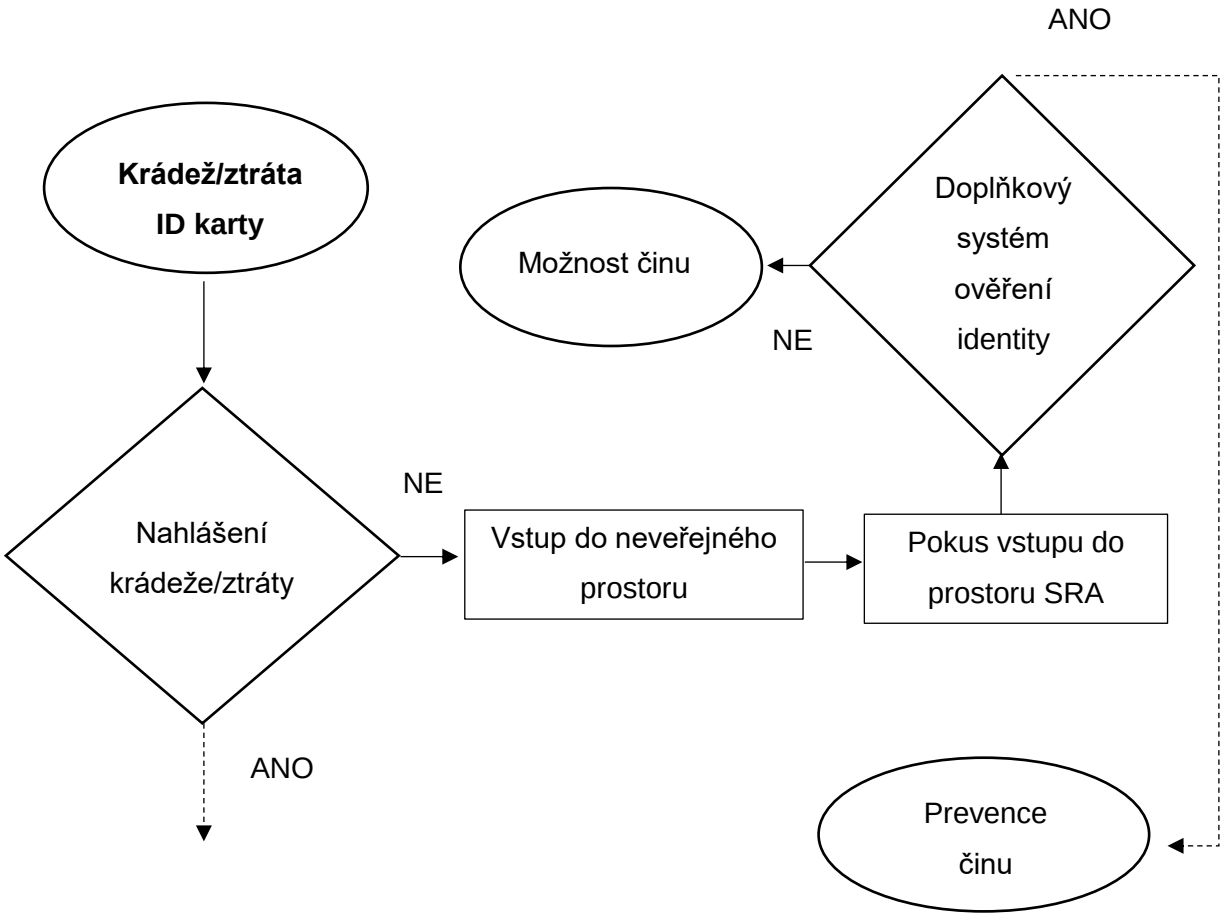
Na blokovém diagramu č 1. je prvním bodem rozhodnutí „nahlášení krádeže nebo ztráty ID karty“. Podle provozovatele letiště zaměstnanec musí při ztrátě či odcizení ID karty její ztrátu nahlásit provozovateli, aby provozovatel mohl ztracenou nebo ukradenou kartu zablokovat v co nejkratším čase. Pokud se tak nestane, hrozí riziko, že neoprávněná osoba může vstoupit do neveřejné části letiště.

Po zablokování ID karty je druhým zásadním bodem v diagramu č. 1 „Systém sledování použití ID karty“ jinými slovy, kam muže být zařazeno hlídaní aktivity ID karty. Systém může upozornit, že ztracená a následně zablokovaná ID karta byla použita k neoprávněnému vstupu. Systém sledování použití by hned hlásil zaměstnancům, kteří se zabývají bezpečností, že byl proveden neoprávněný pokus použití zablokované ID karty. Pokud tento systém není na letišti používán, mohlo by dojít k možnému činu a zároveň by nebylo zjištěno uskuteční pokusu o vstup.



Blokový diagram 1: Krádež nebo ztráta ID karty

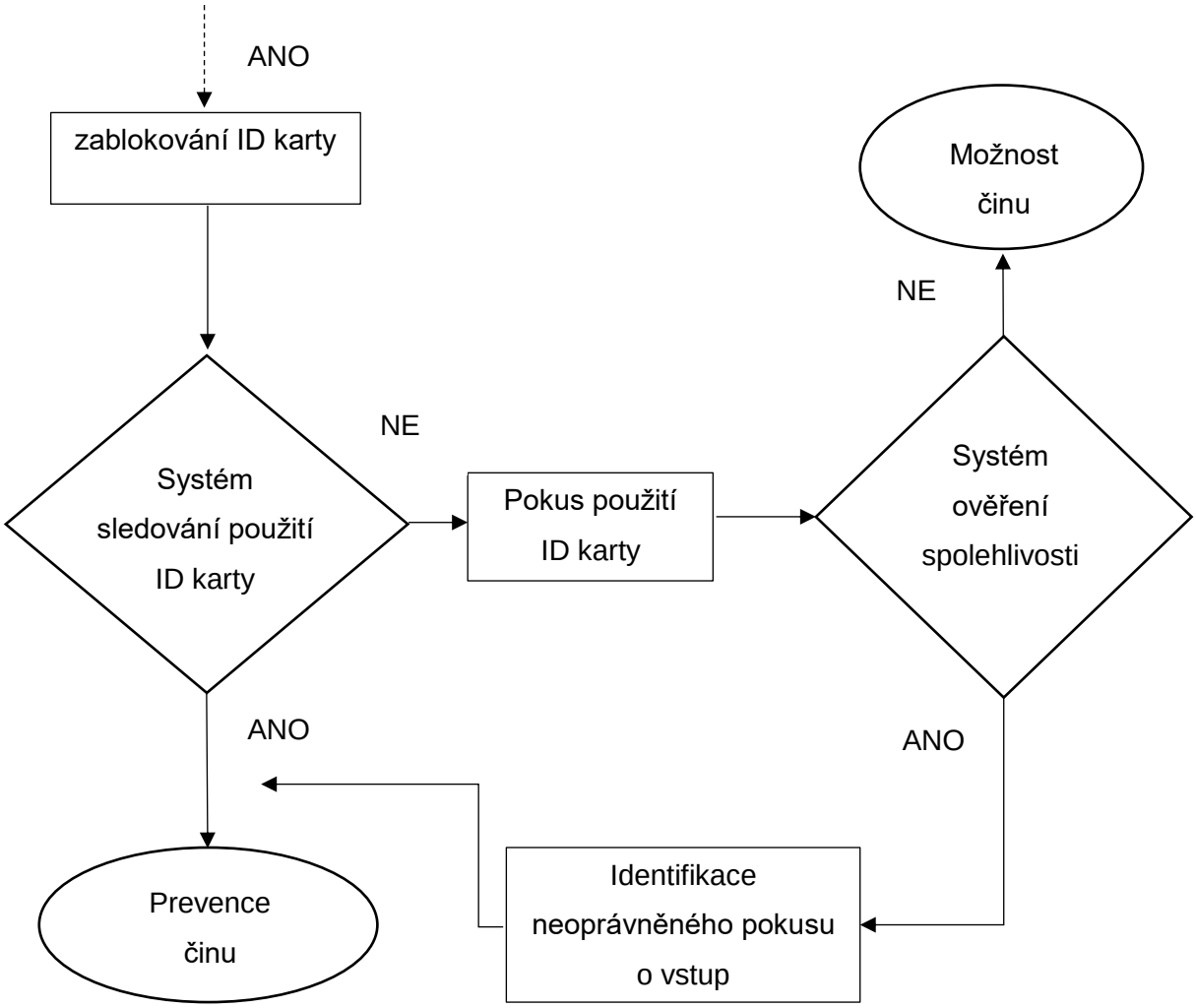
Druhou částí scénáře je přechod mezi neveřejným prostorem a prostorem SRA, nebo přechodem do neveřejného prostoru se zvláštním režimem opatření. Začátek blokového diagramu je úplně stejný (přerušována čára v diagramu znamená, že se jedná o pokračování nebo že se diagram bude pokračovat), jako v předchozím případě viz blokový diagram č. 1. Prvním zásadním bodem je nahlášení ztráty nebo krádeže, kdy v případě nenahlášení může neoprávněná osoba vstoupit do neveřejného prostoru. V případě úspěšného vstupu do neveřejného prostoru se může neoprávněná osoba pokusit o vstup do prostoru SRA nebo do neveřejného prostoru se zvláštním režimem opatření. Mezi průchodem neveřejným prostorem a SRA prostorem může být doplňkový systém ověření identity (tím může být ID karta + systém který by upřesňoval identitu za pomoci doplňkového nástroje). Pokud je systém, který by ověřil identitu neoprávněné osoby v provozu, hned po nepotvrzení identity by byla neoprávněná osoba odhalena a tím by došlo k prevenci činu. V případě, že by doplňkový systém nebyl nainstalován, mohlo by se stát, že neoprávněná osoba vstoupí do prostoru SRA nebo do prostoru se zvláštním režimovým opatřením a může spáchat čin viz blokový diagram č. 2.



Blokový diagram 2: Krádež nebo ztráta ID karty

Dále pokud by po ztrátě nebo krádeže ID karty zaměstnanec ztrátu nahlásil, provozovatel letiště by následně zablokoval kartu, stejně jako v případě prvního scénáře. Pokud došlo k pokusu o použití zablokované karty a nebyl by instalován systém sledování aktivity ID karty,

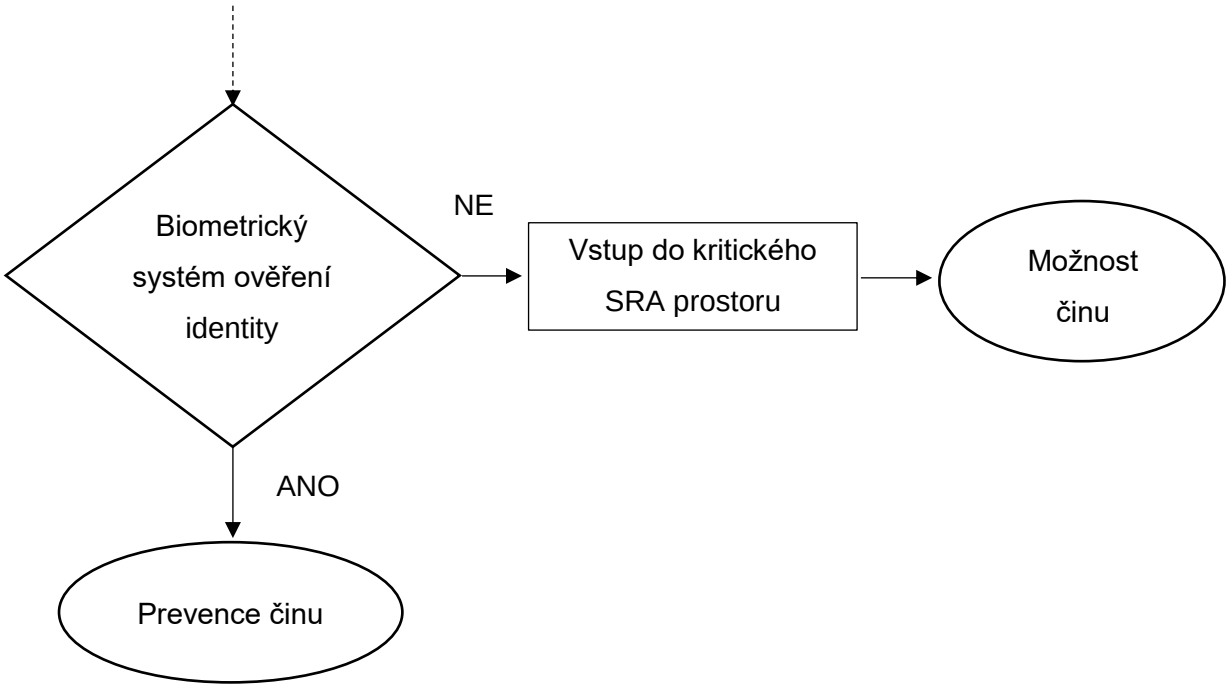
mohlo by dojít k pokusu o využití karty a letištní bezpečnostní systém by nedokázal odhalit pokus o neoprávněný vstup. Teoreticky by mohl být instalován systém ověření spolehlivosti, který by mohl zastavit nebo odhalit pokus o použití. V případě tohoto systému by proběhlo odhalení neoprávněného pokusu použití ID karty zaměstnance letiště a zároveň by došlo k prevenci činu. Pokud by na letiště byl používán „Systém sledování použití ID karty“ stejně jako v první části, systém by hlásil zaměstnancům bezpečnosti letiště neoprávněný pokus o použití ID karty zaměstnance viz blokový diagram č. 3. (přerušována čára v diagramu znamená, že se jedná o pokračování nebo že se diagram bude pokračovat).



Blokový diagram 3:Krádež nebo ztráta ID karty

Třetí část prvního scénáře je přechod mezi SRA prostorem nebo neveřejným prostorem se zvláštním režimovým opatřením a kritickým SRA prostorem. Na tomto typu přechodu je potřeba mít zařízení, které by v žádném případě neumožnilo vstup neoprávněné osoby. V případě prvního scénáře se jedná o krádež nebo ztrátu ID karty. Tento typ přechodu požaduje největší možné zabezpečení, proto není důležitá jednoduchost systému (propustnost) a z toho důvodu by na daném přechodu mohl být použit systém ověření identity

pomocí biometrických údajů viz blokový diagram č. 4 (přerušována čára v diagramu znamená, že se jedná o pokračování nebo že se bude diagram pokračovat). Tím může být otisk prstu, geometrie obličeje nebo skenovaní sítnice oka.



Blokový diagram 4:Krádež nebo ztráta ID karty

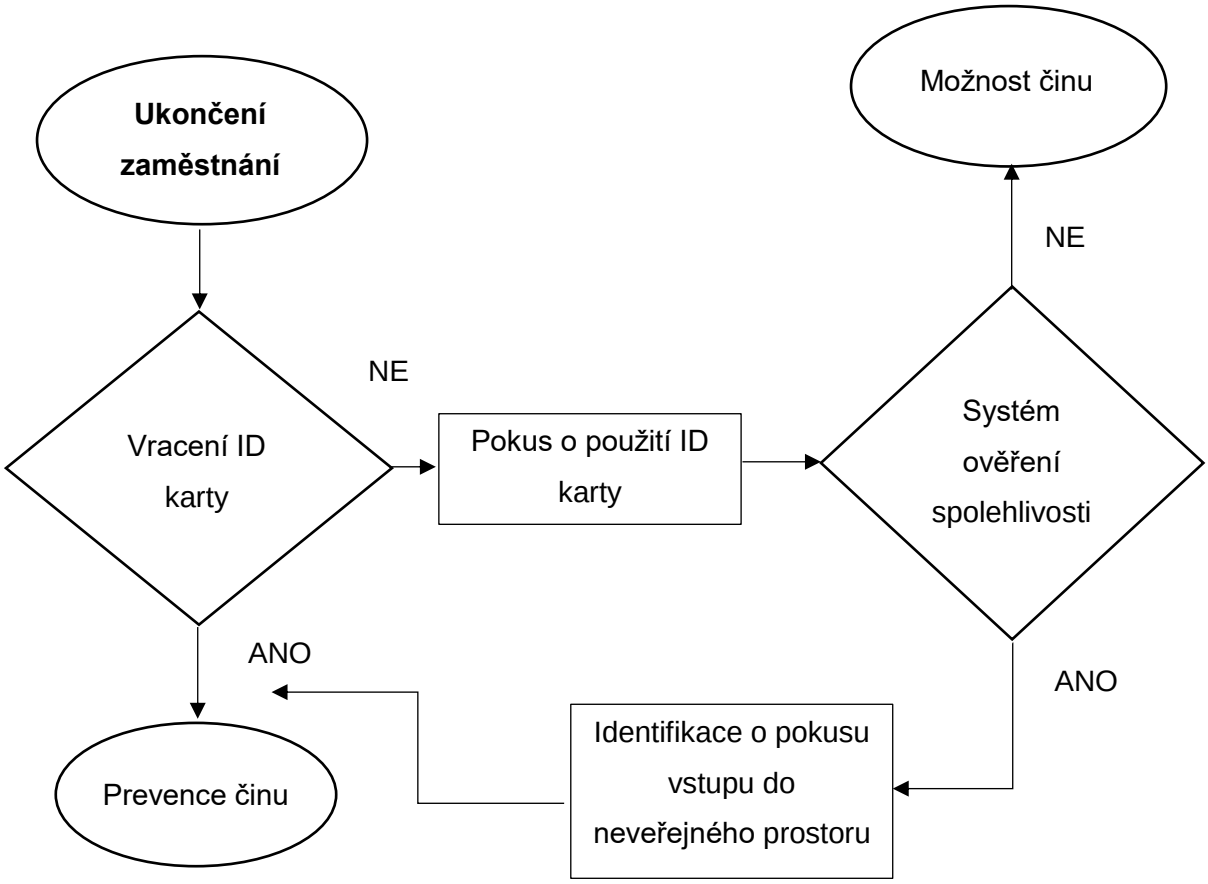
5.1.2 Ukončení zaměstnaní

Druhým scénářem je ukončení zaměstnání. Je to velice důležitý typ scénáře. Zásadní bod scénáře je použití staré ID karty zaměstnance pro neoprávněný vstup do neveřejné části letiště.

Například na letišti Václava Havla v Praze vrácení ID karty probíhá tím způsobem, že zaměstnanec po ukončení pracovního poměru nebo po výzvě provozovatele letiště musí odevzdat ID kartu, pokud nedošlo k odevzdání po opakované výzvě, jedná se o případ podezření ze spáchání přestupku dle paragrafu §92a zákona č. 49/1997 Sb. [12]

První část druhého scénáře je přechod mezi veřejným a neveřejným prostorem viz Blokový diagram č. 5. Hlavním bodem je „Vrácení ID karty“ provozovateli letiště. Pokud bývalý zaměstnanec neodevzdal ID kartu během doby, která je vyhrazena pro vrácení ID karty, může dojít k tomu, že osoba, která ukončila zaměstnání může použít kartu. Pokud zaměstnavatel nahlásil ukončení zaměstnání konkrétní osoby provozovateli letiště, jde pouze o kontrolu vrácení – nemůže dojít k činu. Pokud ale zaměstnanec ukončil zaměstnání a zaměstnavatel nenahlásil provozovateli letiště, že konkrétní zaměstnanec už by neměl mít přístup do neveřejných letištních prostorů, může dojít k činu.

Nahlášení o ukončení zaměstnání osoby zaměstnavatelem provozovateli letiště můžeme pojmenovat v první části druhého scénáře, jako druhý zásadní bod – „systém ověření spolehlivosti“.



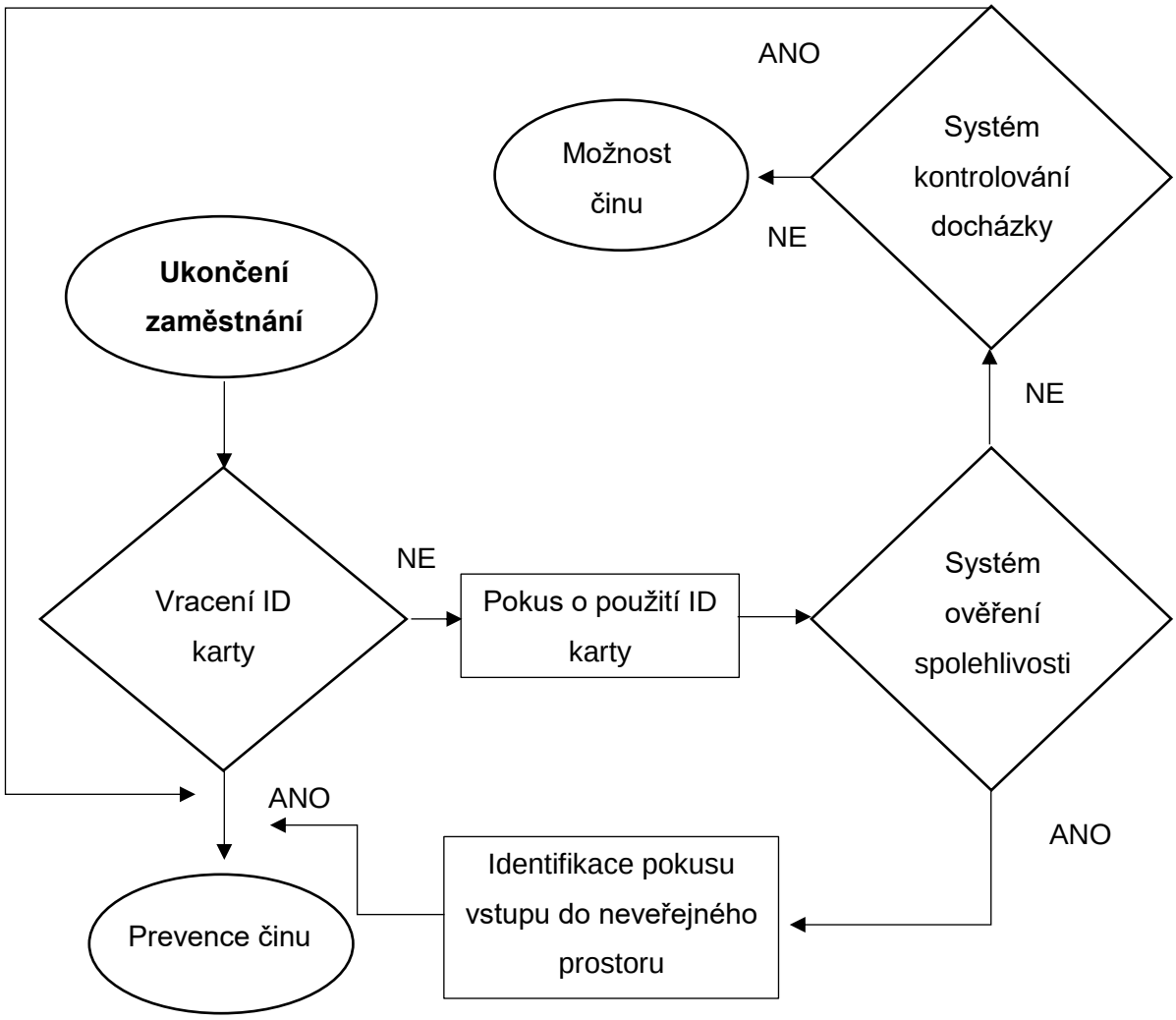
Blokový diagram 5: Ukončení zaměstnání

Ve druhé části scénáře se jedná o přechod mezi neveřejnou částí letiště a prostorem SRA nebo prostorem se zvláštním režimovým opatřením, který je znázorněný v blokovém diagramu č 6. Začátek blokového diagramu č. 6 je jako v blokovém diagramu č. 5, a také hlavním bodem je „Vrácení ID karty“.

Pokud zaměstnanec nevrátil kartu po ukončení zaměstnání, ověřuje se oprávněnost přístupu pomocí „systému ověření spolehlivosti“, stejně jako v první části druhého scénáře. Pokud není „systém ověření spolehlivosti“ a na dalším přechodu není používán doplňkový systém, který by mohl zkontrolovat potřebnou přítomnost na daném úseku osoby, která se pokouší o vstup, mohlo by dojít k činu na daném úseku nebo o pokus o vstup do dalšího neveřejného prostoru. Pokud je na přechodu z neveřejné časti do SRA prostoru nebo neveřejného prostoru se zvláštním režimovým opatřením systém, který by kontroloval potřebnou přítomnosti v současnou chvíli: například „systém kontrolování docházky“. V tom případě by nedošlo k neoprávněnému vstupu do prostoru SRA nebo do neveřejného prostoru se zvláštním režimovým opatřením, ale došlo by pouze k neoprávněnému pokusu o vstup.

Bezpečnostnímu pracovníkovi letiště by hned bylo jasné, že osoba, která už nemá oprávněný vstup, se o něj pokouší a tím by došlo k prevenci činu.

Pokud ale není používán žádný systém, který by kontroloval potřebnou přítomnost na přechodu mezi veřejnou a neveřejnou částí, a pokud je též nepoužíván systém na druhé úrovni přestupu, což je přechod z neveřejné části do SRA prostoru nebo do neveřejného prostoru se zvláštním režimovým opatřením může dojít k činu.



Blokový diagram 6:Ukončení zaměstnání

Ve třetí části druhého scénáře viz blokový diagram č 7. je znázorněn možný scénář toho, co by se mohlo stát, pokud by se osoba po ukončení zaměstnání pokoušela využít ID kartu, kterou využívala v době svého zaměstnání. Začátek scénáře je stejný (přerušována čára v diagramu znamená, že se jedná o pokračování nebo že se bude diagram pokračovat), jako v předchozím případě je scénář znázorněn na blokových diagramech č. 5 a č. 6. Velmi záleží na první a druhé části druhého scénáře, záleží totiž, jestli zaměstnavatel nahlásí, že zaměstnanec už nemá povolení na vstup a provozovatel letiště ID kartu zablokuje.

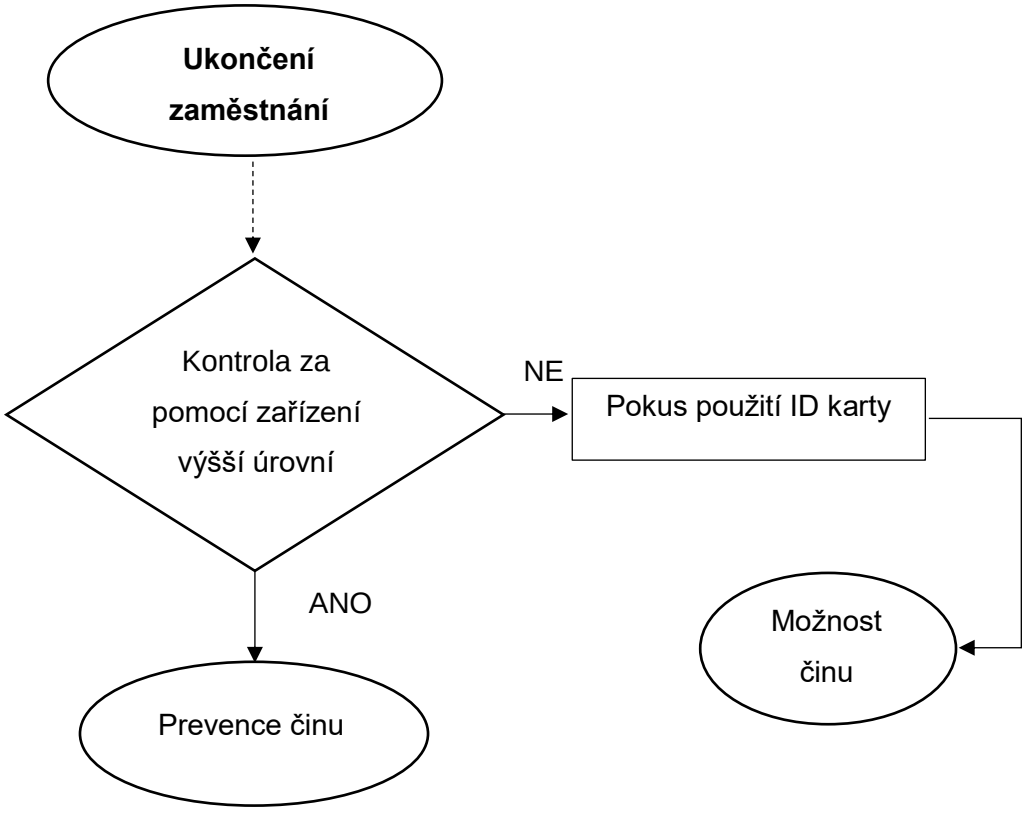
Pro zjištění nejhorší možné situace, která může nastat, budeme předpokládat nejhorší variantu – nenahlášení a ukončení zaměstnání a taky situace, že se neoprávněné osobě podařilo projít přes dvě předchozí kontroly.

Ve třetí části druhého scénáře se jedná o přechod mezi SRA prostorem nebo neveřejným prostorem se zvláštním režimovým opatřením a kritickým SRA prostorem.

Kritický SRA prostor je prostor s velmi vysokou úrovní opatření. V žádném případě nemůže dojít k tomu, aby se neoprávněná osoba pohybovala v tomto prostoru. Vzhledem k tomu, že jsou zvažovány všechny možné scénáře, teoreticky lze říct, že k pohybu v prostoru kritického SRA může dojít. K vstupu může dojít v případě, že není žádné zabezpečení mezi SRA prostorem a kritickým SRA prostorem anebo mezi neveřejným prostorem se zvláštním režimovým potřením a kritickým SRA prostorem. Může dojít k tomu, že na daném přechodu jsou používaná zabezpečení, která fungují stejným způsobem, jako na předchozích přechodech. Stejná funkce znamená, že zařízení nemá naprogramovanou informaci o tom, že konkrétní osoba ukončila zaměstnání a už nemá oprávněný přístup.

Zajistit prevenci činu by mohlo zařízení, které by provádělo kontrolu na jiné úrovni, a to na úrovni vyšší než na předchozích typech přestupu. Například by to mohlo být zařízení, které by kontrolovalo identitu pomocí biometrických údajů viz blokový diagram č. 7.

Největším problémem druhého scénáře je komunikace mezi zaměstnavatelem a provozovatelem letiště.

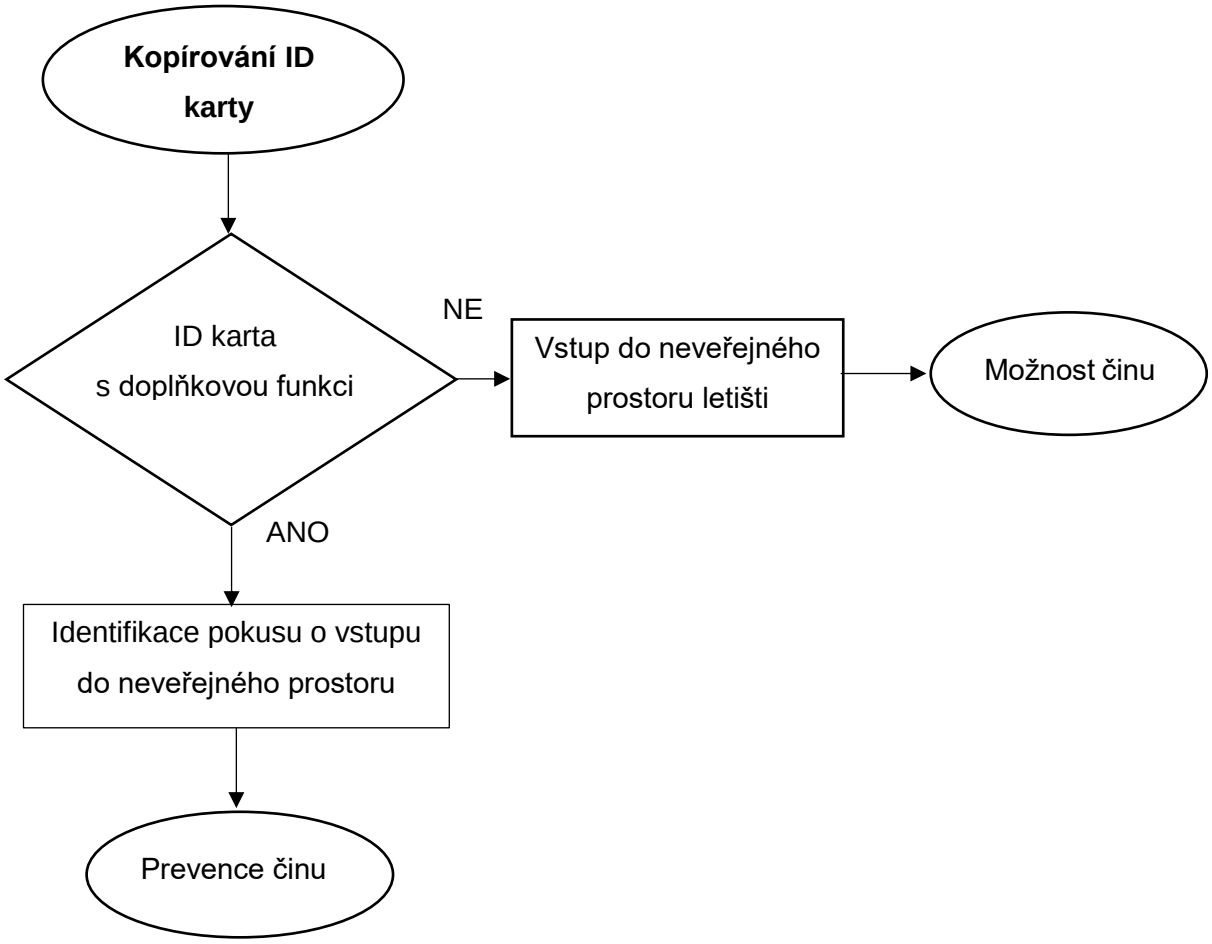


Blokový diagram 7: Ukončeni zaměstnaní

5.1.3 Kopírování ID karty

Třetím scénářem je „kopírovaní ID karty“. Kopírování ID karty může být prováděno několika způsoby viz kapitola 4.6. Při návrhu bezpečnostního systému je zásadní otázka na bezpečnost letiště, ale důležitou roli hraje taky ekonomické hledisko, protože bezpečnostní systém s využitím ID karet je přímo úměrný ceně bezpečnostního systému. Proto je velice důležité rozhodnout o využití velmi dobře zabezpečených ID karet nebo o využití ID karet s doplňkovým systémem ověření identity. Právě proto by hlavním zařízením, které by mělo chránit neoprávněný vstup do neveřejných prostorů letiště, měly být různé systémy spojené s identifikací. Mohou to být systémy, které by pracovaly spolu s ID kartou, například ID karta + unikátní kód anebo systémy podporující identifikaci osoby pomocí biometrických údajů. Na druhé straně ale vždy bude požadavek na určitou propustnost na jednotlivých úsecích při kontrole.

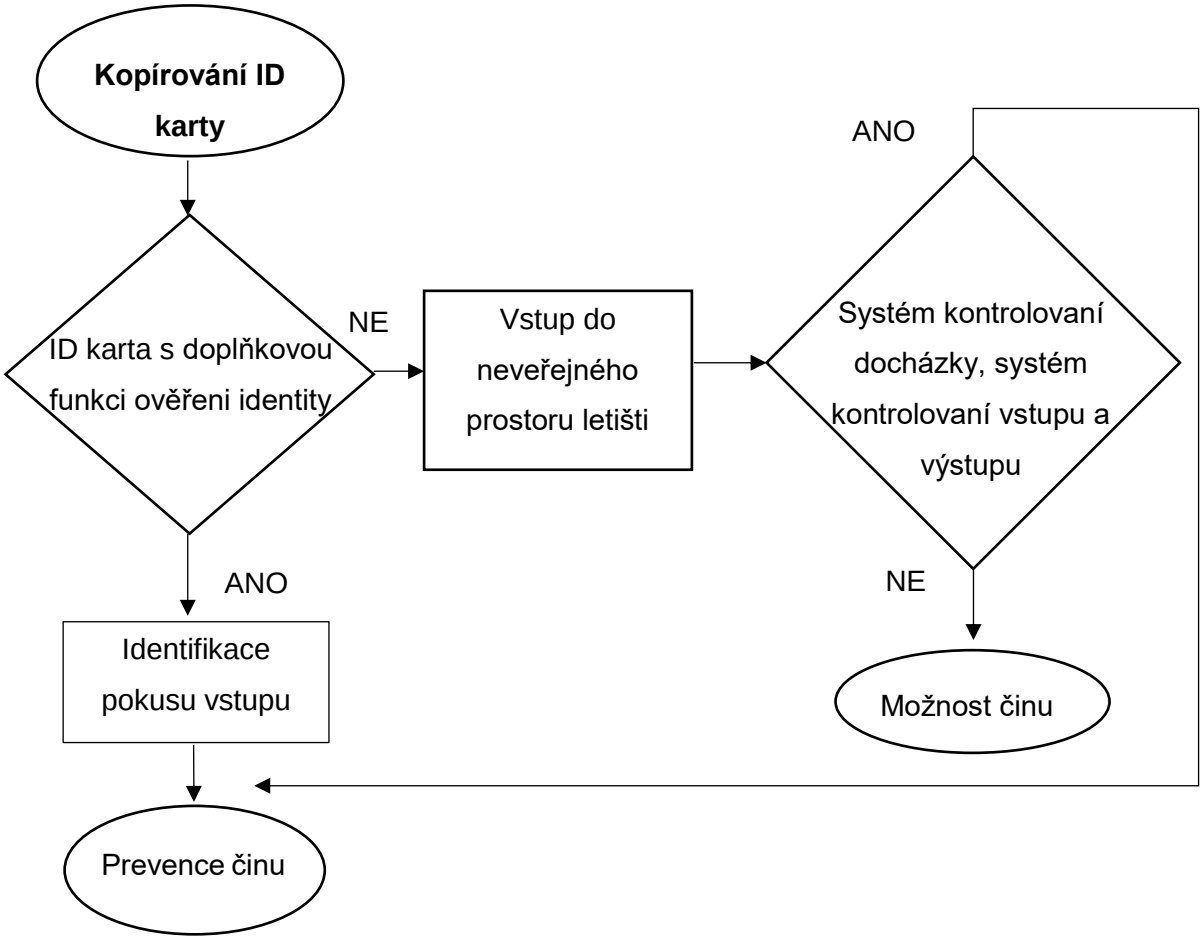
V případě první části třetího scénáře, se jedná o přechod z veřejného prostorou do neveřejného prostoru letiště. Je to první přechod a je využívanější, než přechod mezi neveřejným prostorem a SRA prostorem, prostorem neveřejným a neveřejným prostorem se zvláštním režimovým opatřením, mezi SRA prostorem a kritickým SRA prostorem a taky mezi neveřejným prostorem se zvláštním režimovým opatřením a kritickým SRA prostorem. Proto na přechodu mezi veřejným a neveřejným prostorem musí být využita technologie, která by mohla ověřit identitu nejrychlejším možným způsobem. To může být například jen čtečka pro ID kartu, která po přiložení nebo po vložení do čtečky zkontroluje přístup k přechodu mezi prostory a v případě, že osoba má oprávněný vstup, povolí přístup do další zóny. V případě kopírování ID karty by nestačilo ověření jen pomocí ID karty, ale bylo by lepší využít ID karty spolu s doplňkovým systém kontroly identity. Je to dobře vidět na blokovém diagramu č. 8. Pokud v první části tohoto scénáře bude zařízení s doplňkovou funkcí ověření identity, dojde k identifikace pokusu vstupu do neveřejného prostoru a případné prevenci činu. Pokud by nebyla instalovaná doplňková funkce, mohl by proběhnout vstup do neveřejného prostoru letiště a tak by mohlo dojít k činu na území neveřejného prostoru letiště.



Blokový diagram 8: Kopírování ID karty.

Druhou částí třetího scénáře je přechod mezi neveřejným prostorem letiště a prostorem SRA a též přechod mezi neveřejným prostorem a neveřejným prostorem se zvláštním režimovým opatřením. Tyto typy přechodů požadují zvýšenou bezpečnost a kontrolu na vyšší úrovni, a to vzhledem k tomu, že se jedná o typy přechodů s menší propustností (to znamená, že přechod využívá menší počet lidí). Přechod využívají jen osoby, které mají povolení vstupu do SRA prostoru a neveřejného prostoru se zvláštním režimovým opatřením. Právě na této úrovni by bylo možné využít zařízení, které by mohlo ověřit identitu zaměstnance při použití delšího času, protože tento typ bezpečnosti přechodu vyžaduje zvýšenou úroveň bezpečnosti. Blokový diagram č. 9. má stejný začátek jako blokový diagram č. 8 v první části třetího scénáře. Rozhodující bod pak nastává právě při druhém stupni kontroly, kdy se jedná o několik zařízení, které by mohly odhalit pokus o neoprávněný vstup. Mohlo by se jednat o jednoduchá zařízení, která byla zmíněna výše: systém kontrolování potřebné přítomnosti (jinak řečeno systém docházky), který by informoval bezpečnostní pracovníky letiště o tom, zda se osoba v současné chvíli nachází na území neveřejné části letiště. Nebo se může jednat o systém kontrolování vstupu a výstupu, což znamená, kolik bylo uskutečněno výstupů a vstupů konkrétní osoby v daném časovém intervalu.

Aby byla umožněna prevence toho, že pro vstup byla karta použita vícekrát, než byl uskutečněn výstup, a také aby v omezeném časovém intervalu nedocházelo k většímu počtu vstupů a výstupů za sebou, je nutné instalovat zařízení, která by mohla na daném typu přechodu ověřit identitu pomocí jednoduchého kódu nebo použitím biometrických údajů.
Pokud by byly ukradeny údaje zaměstnanců společně s jednotlivými bezpečnostními kódy, jediné, co by mohlo pozastavit hrozbu vniknutí do prostoru, je kontrolování bezpečnostním pracovníkem letiště ID karty. Docházelo by k porovnání fotografie na ID kartě, kontrolování data platnosti, názvu zaměstnavatele a povolení vstupu do prostoru, do kterého se osoba pokouší vstoupit.
Pokud by byl zaveden systém kontrolování identity pomocí shody biometrických údajů, došlo by okamžitě k odhalení neoprávněného pokusu o vstup do neveřejné části letiště. Pokud by nebyl zaveden biometrický systém, jediné, co by mohlo vést k prevenci činu, je dobrá práce a pozornost zaměstnance bezpečnostní kontroly letiště.
Kdyby všechny výše zmíněné faktory neexistovaly, tak by došlo k neoprávněnému vstupu do SRA prostorou nebo do neveřejného prostoru se zvláštním režimovým opatřením a poté by mohlo dojít k činu.



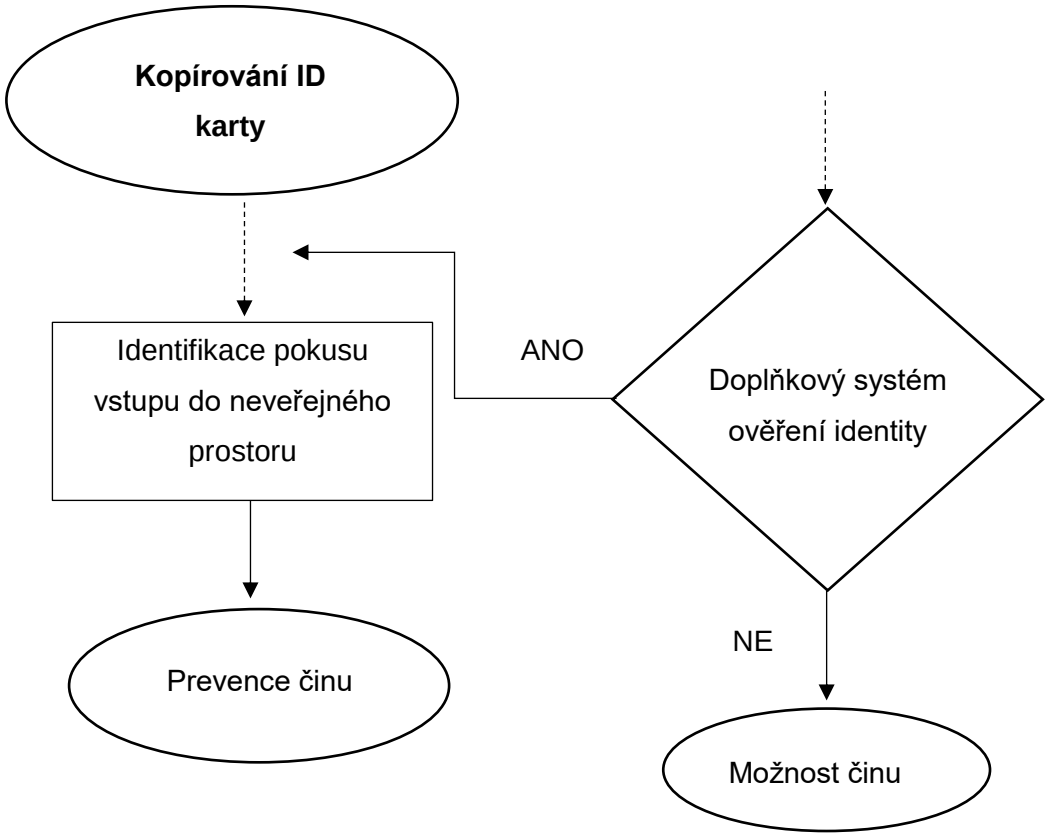
Blokový diagram 9: Kopírování ID karty.

Na blokovém diagramu č. 9 je znázorněna problematika mezi přestupy z SRA prostoru do kritického SRA prostoru nebo z neveřejného prostorou se zvláštním opatřením do kritického SRA prostorou. Začátek blokového diagramu je úplně stejný jako v první a druhé části třetího scénáře „kopírování ID karty“ (přerušována čára v diagramu znamená, že se jedná o pokračování nebo že se bude diagram pokračovat), přičemž hlavní rozdíl je v tom, že by žádným způsobem nemělo dojít k neoprávněnému vstupu do kritického prostorou SRA.

V tomto případě není důležitý čas, který by byl použit na kontrolu. Hlavním cílem je zde bezpečnost. Aby nedošlo k neoprávněnému pohybu na území prostoru kritická SRA, je vhodné použít nejspolehlivější systémy pro ověření identity.

Jiný problém může nastat ve chvíli, kdy kopírování proběhlo na úrovni systému, to znamená, že systém byl zneužit hackery, kteří by mohli povolit vstup na jakékoliv úrovni přechodu. Jediné, co by zneužití mohlo zachránit je zálohování systému, lidský faktor a zálohový systém ověření identity.

Lidským faktorem je myšlena, spolehlivost zaměstnance bezpečnostní kontroly, pozornost a profesionálnost. Zálohovým systémem rozumíme systém, který by byl vždy nezávislý a funkční i v případě výpadku nebo útoku hackerů na celý letištní bezpečnostní systém.



Blokový diagram 10:Kopírování ID karty.

6 Matematický model detekce pohybu neoprávněné osoby mezi neveřejnými prostory

V kapitole č. 5 jsme probírali různé typy scénářů, které popisovaly problematiku bezpečnostního systému a co by se mohlo stát na určitých úsecích v případě, že by nebylo používáno správné zařízení pro detekování neoprávněného vstupu.

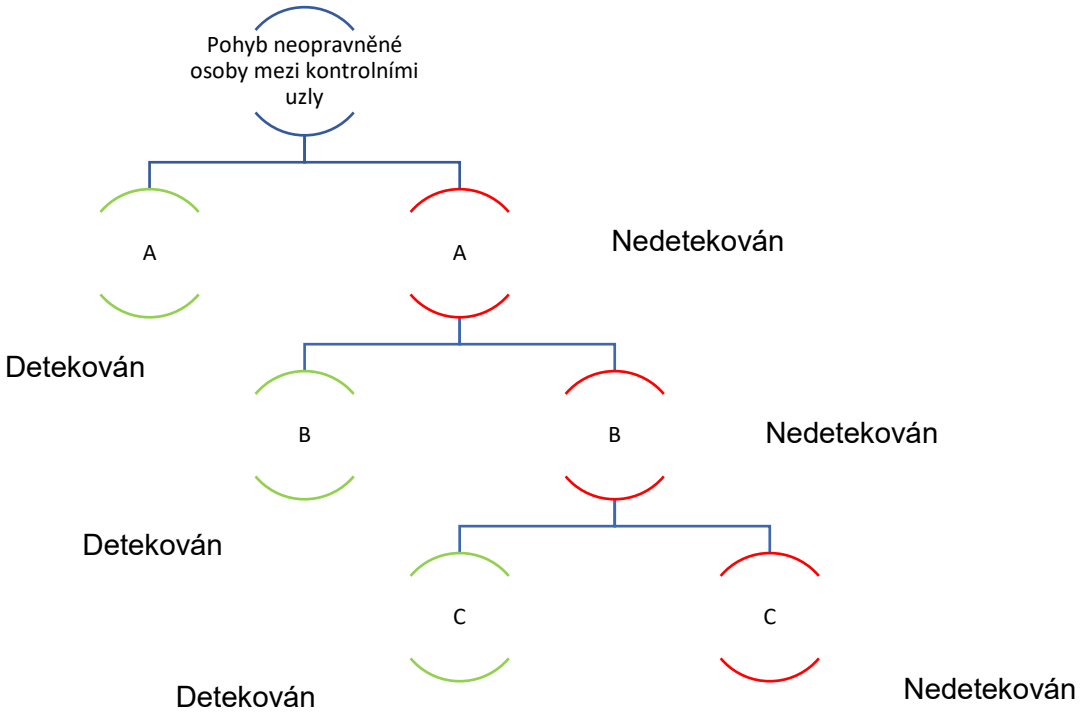
Vzhledem k tomu, že všechny scénáře probíhají mezi stejnými prostory, můžeme spočítat obecnou pravděpodobnost nedetekování průchodu neoprávněné osoby mezi neveřejnými prostory.

Proces bezpečnostní kontroly zaměstnanců s neoprávněným vstupem zahrnuje:

- přechod mezi veřejnou a neveřejnou částí (uzel A)
- přechod mezi neveřejným prostorem a SRA prostorem nebo neveřejným prostorem se zvláštním režimovým opatřením (uzel B)
- přechod mezi SRA prostorem nebo neveřejným prostorem se zvláštním režimovým opatřením a kritickým SRA prostorem (uzel C)

Možné události viz obrázek č. 13.

1. Neoprávněná osoba je detektována na uzlu A
2. Neoprávněná osoba není detektována na uzlu A
3. Neoprávněná osoba je detektována na uzlu B
4. Neoprávněná osoba není detektována na uzlu B
5. Neoprávněná osoba je detektována na uzlu C
6. Neoprávněná osoba není detektována na uzlu C



Obrázek 13: Detekce neoprávněného vstupu na určitých uzlech

6.1 Pravděpodobnost nedetekování neoprávněné osoby

Pro výpočet pravděpodobnosti nedetekovaní průchodu mezi prostory neoprávněné osoby můžeme využit Binomické rozdělení. Binomické rozdělení je rozložení počtu „úspěšných průchodů“ v posloupnosti **n** (pokusů)**,** které jsou závislé na náhodných experimentech tak, že pravděpodobnost „úspěchu průchodů“ v každém z nich je konstantní a rovná se **p** viz vzorec č. 6. 1.

$$P = [X = X] = \binom{n}{x} * p^x * (1-p)^{n-x} \tag{6.1}$$

kde $\binom{n}{x}$ je binomický koeficient viz vzorec č. 6. 2.

$$\binom{n}{x} = \frac{n!}{k! * (n-k)!} \tag{6.2}$$

- Diskrétní náhodná veličina **X** s binomickým rozdělením může nabývat celočíselných hodnot od 0 do **n**.
- Pravděpodobnost, že jev nastane **x**krát z **n** pokusů při pravděpodobnosti jevu **p**.

Pro výpočet předpokládám pravděpodobnost **p**, že neoprávněná osoba nebyla detekována, nezávisle na okamžité poloze.

Pravděpodobnost, že neoprávněná osoba byla detekována je pak**1-p.**

V našem případě můžeme využit binomickou distribuci, protože je známý počet možných událostí, jejichž pravděpodobnost zjišťujeme. Potom pravděpodobnost dána vzorcem č. 6. 3.

$$P = \binom{n}{k} * p^k * (1-p)^{n-k} = \binom{n}{k} = \frac{n!}{k! * (n-k)!} * p^k * (1-p)^{n-k} \quad (6.3)$$

6.1.1 Možné případy nedetekování na určitých bezpečnostních uzlech:

1) nebyl detektován na uzlu A (k=1), jeden z třech možných pokusu (n=3)
2) nebyl detektován na uzlu B (k=2), jeden z třech možných pokusu (n=3)
3) nebyl detektován na uzlu C (k=3), jeden z třech možných pokusu (n=3)

6.1.1.1 Nedetekování na přechodu mezi veřejným a neveřejným prostorem

Prvním případem je pokus o vstup do neveřejného prostoru (uzel A), přičemž celkem jsou možné tři pokusy, proto k =1, n=3.

Po aplikování binomické distribuce, je P_A pravděpodobnost, že neoprávněná osoba nebyla detekována na uzlu A viz vzorec č. 6. 4.

$$P_A = \frac{n!}{k! * (n-k)!} * p^k * (1-p)^{n-k} = \frac{3!}{1! * 2!} * p^1 (1-p)^2 \quad (6.4)$$

Po dosažení do vzorce č. 6. 4 hodnoty k=1 a n=3, pak dojdeme k rovnice č. 6. 5.

$$P_A = 3 * p - 6 * p^2 + 3 * p^3 \quad (6.5)$$

Výslednou funkci můžeme řešit pro dvě okrajové podmínky: pro P_A=1 a P_A=0

1) P_A=1

$$P_A = 3 * p - 6 * p^2 + 3 * p^3 \quad (6.6)$$

Pro řešení kubické rovnice, lze použít teorii Vieta - Kardana. [22]

Pro odvození řešení je potřeba využít kubickou rovnici v základním tvaru viz vzorec č. 6. 7:

$$x^3 + a * x^2 + b * x + c = 0 \quad (6.7)$$

Řešení spočívá v tom, že je potřeba vypočítat hodnoty Q, R, S, (viz vzorci 6. 8, 6. 9 a 6.10) a φ (φ se se počítá na základě výsledku hodnoty S, jestli je vetší, rovná se nebo je menší než 0. V našem výpočtu se setkáme jen s hodnotou S, která je menší než 0):

$$Q = \frac{a^2 - 3 * b}{9} \tag{6.8}$$

$$R = \frac{2 * a^3 - 9 * a * b + 27 * c}{54} \tag{6.9}$$

$$S = Q^3 - R^2 \tag{6.10}$$

Dále v řešení nastává důležitý moment, a to jestli hodnota S>0, S<0 nebo S=0. Od této podmínky se bude odvíjet řešení.

Nejdříve musíme rovnice č. 6. 6 upravit do tvaru viz rovnice č. 6. 11.

$$3 * p - 6 * p^2 + 3 * p^3 - 1 = 0 \tag{6.11}$$

Po úpravě rovnice č. 6. 11 nám vyplyne rovnice č. 6. 12:

$$p^3 - 2 * p^2 + p - \frac{1}{3} = 0 \tag{6.12}$$

Nyní už rovnice č. 6. 12 má stejný základní vzhled jako rovnice podle teorie Vieta - Kardana. Je tedy možné dosadit do původních vzorců (vzorce č. 6. 8,6. 9 a 6.10) hodnoty kubické rovince, kterou je potřeba spočítat viz rovnice č. 6. 13, 6. 14, 6. 15.

$$Q = \frac{a^2 - 3 * b}{9} = \frac{(-2)^2 - 3}{9} = 0{,}11 \tag{6.13}$$

$$R = \frac{2 * a^3 - 9 * a * b + 27 * c}{54} = \frac{2 * 2^3 - 9 * 2 * 1 + 27 * \frac{1}{3}}{54} = -0{,}13 \tag{6.14}$$

$$S = Q^3 - R^2 = 0{,}11^3 - (-0{,}13)^2 = 0{,}001331 - 0{,}0169 = -0{,}015 \tag{6.15}$$

Vzhledem k tomu že S<0 a Q>0 musíme pro výpočet využít (vzorce č. 6. 16, 6. 17 a 6. 18):

$$\varphi = \frac{1}{3}\mathrm{Arch}\left(\frac{|R|}{\sqrt{Q^3}}\right) \tag{6.16}$$

$$p_1 = -2sgn(R)\sqrt{Q}ch(\varphi) - \frac{a}{3} \tag{6.17}$$

$$p_{2,3} = sgn(R)\sqrt{Q}ch(\varphi) - \frac{a}{3} \pm i\sqrt{3}\sqrt{Q}sh \tag{6.18}$$

Podle trigonometrického odvozování Vieta - Kardana, kde p_1 bude reálné číslo, kořeny $p_{2,3}$ budou komplexními čísly, které pro řešení nepotřebujeme. Pro výpočet p_1 budeme potřebovat φ viz vzorec č. 6.19:

$$\varphi = \frac{1}{3}\mathrm{Arch}\left(\frac{|R|}{\sqrt{Q^3}}\right) = \frac{1}{3}\mathrm{Arch}\left(\frac{|-0{,}13|}{\sqrt{0{,}11^3}}\right) = 0{,}642 \tag{6.19}$$

Pak je možné vypočítat p_1 (vzorec č. 6. 20):

$$p_1 = -2sgn(R)\sqrt{Q}ch(\varphi) - \frac{a}{3} = -2sgn(-0{,}13)\sqrt{0{,}11}ch(0{,}65) = 1{,}48 \tag{6.20}$$

V našem případě bude výsledek p_1 = 1,48 což je z hlediska pravděpodobnosti nereálné řešení.

2) Ve druhém případě budeme počítat, že pravděpodobnost nedetekování P_A=0 viz vzorec č. 6. 5:

$$P_A = 3 * p - 6 * p^2 + 3 * p^3 \tag{6.21}$$

Ze vzorce č. 6. 21 úpravou dostaneme rovnice č. 6. 22:

$$3 * p - 6 * p^2 + 3 * p^3 = 0 \tag{6.22}$$

Pro řešení rovnice č. 22 můžeme využít klasické řešení kvadratické rovnice. Abychom mohli využít řešení pomocí kvadratické rovnice, musíme nejdříve rovnice č. 6. 22 upravit do potřebného tvaru. Z rovnice č. 6. 22 můžeme vytknout 3*p. Poté budeme muset vyřešit dvě rovnice (rovnici č. 6. 22 a 6. 24):

$$3 * p * (1 - 2 * p + p^2) = 0 \tag{6.23}$$

První rovnice je 3*p=0, řešením je tedy 0. Je to jediné reálné řešení rovnice. Řešení druhé rovnice viz rovnice č. 6. 24 je p=1, přičemž pro řešení rovnice jsme využili výpočet přes diskriminant.

$$1 - 2 * p + p^2 = 0 \tag{6.24}$$

6.1.1.2 Nedetekovaní na přechodu mezi neveřejným prostorem a SRA prostorem nebo neveřejným prostorem se zvláštním režimovým opatřením

Jedná se o pokus detekce na přechodu B, viz obrázek č. 13. Pro výpočet pravděpodobnosti nedetekovaní na uzlu B budeme také využívat binomické rozdělení, viz rovnice č. 6. 25. V tomto případě bude n=3 a k=2, protože se jedná o druhý pokus ze třech možných.

$$P_B = \frac{n!}{k! * (n-k)!} * p^k * (1-p)^{n-k} = \frac{3!}{2! * 1!} * p^1(1-\mathrm{p}) = 3 * p^2 - 3 * p^3 \quad (6.25)$$

Výslednou funkci (viz rovnice č. 6. 26), funkci pravděpodobnosti můžeme řešit pro dvě okrajové podmínky: pro P_B=1 a P_B=0.

$$P_B = 3 * p^2 - 3 * p^3$$

1) Prvním případem je P_B=1, kdy po úpravě rovnic č. 6. 27 a 6. 28 (6.26)

$$P_B = 3 * p^2 - 3 * p^3 = 1 \quad (6.27)$$

$$3 * p^2 - 3 * p^3 - 1 = 0 \quad (6.28)$$

Pro tento případ také můžeme využít teorému Vieta - Kardana pro výpočet kořenu u kubické rovnice. Podle teorémy potřebujeme najít Q, R, S a φ (viz vzorce č. 6. 29, 6. 30 a 6. 31).

$$Q = \frac{a^2 - 3 * b}{9} = \frac{3^2 - 3 * 0}{9} = 0{,}11 \quad (6.29)$$

$$R = \frac{2 * a^3 - 9 * a * b + 27 * c}{54} = \frac{2 * 3^3 - 9 * 3 * 0 + 27 * (-1)}{54} = 0{,}13 \quad (6.30)$$

$$S = Q^3 - R^2 = 0{,}11^3 - 0{,}13^2 = -0{,}015 \quad (6.31)$$

Vzhledem k tomu, že S<0 a Q>0 pro výpočet ve druhém případě také musíme využít vzorec č. 6. 32:

$$\varphi = \frac{1}{3}\mathrm{Arch}\left(\frac{|R|}{\sqrt{Q^3}}\right) \quad (6.32)$$

Pak dostaneme pro p_1, p_2 a p_3 viz vzorce č. 6. 33 a 6. 34:

$$p_1 = -2sgn(R)\sqrt{Q}ch(\varphi) - \frac{a}{3} \quad (6.33)$$

$$p_{2,3} = sgn(R)\sqrt{Q}ch(\varphi) - \frac{a}{3} \pm i\sqrt{3}\sqrt{Q}sh(\varphi) \quad (6.34)$$

Při dosazení všech hodnot do rovnic č. 6. 32, 6. 33, 6. 34. nám vyjde, že p_1=-0,47, což je záporný kořen a je to nereálné řešení. Ostatní kořeny $p_{2,3}$ jsou komplexní řešení, což je také považováno za nereálné řešení.

2) Druhý případ počítáme, že pravděpodobnost nedekování na uzlu B je P_B=0. Po úpravě dostaneme vzorce č. 6. 35 a 6. 36:

$$P_B = 3 * p^2 - 3 * p^3 = 0 \tag{6.35}$$

$$3 * p^2 - 3 * p^3 = 0 \tag{6.36}$$

Pro řešení rovnici č. 6. 36 můžeme vytknout 3*p^3, poté budeme moci jednoduše vyřešit dvě rovnice a to jsou rovnice č. 6. 37 a rovnice č. 6. 38.

$$3 * p^3 = 0 \tag{6.37}$$

$$1 - p = 0 \tag{6.38}$$

Výsledkem rovnice č. 6. 37 je p=0, což je reálné řešení, řešeni rovince č 38 je p=1.

6.1.1.3 Nedetektovaní na přechodu mezi SRA prostorem nebo neveřejným prostorem se zvláštním režimovým opatřením a kritickým SRA prostorem

V tomto případě se jedná o nedetekování na uzlu C, viz obrázek č. 13. Pro výpočet pravděpodobnosti nedetekovaní na uzlu C, také jak v předchozích případech viz kapitola č. 6.1.1.1 a kapitola č. 6.1.1.2 budeme využívat binomické rozdělení viz rovnice č. 6. 25. Ale v posledním to případě n=3 a k=3, protože se jedná o třetí pokus ze třech možných.

$$P_C = \frac{n!}{k! * (n-k)!} * p^k * (1-p)^{n-k} = \frac{3!}{3! * 0!} * p^3 (1-p)^0 = p^3 \tag{6.39}$$

Výslednou funkci pravděpodobnosti P_C můžeme považovat za úroveň kvality bezpečnostního systému letiště, protože prostor kritické SRA je poslední místo, kam se může dostat neoprávněná osoba.

$$P_C = 3 * p^2 - 3 * p^3 \tag{6.40}$$

6.2 Výsledek ze spočtené pravděpodobnosti

Abychom mohli zjistit optimální pravděpodobnost „p“ při nedetekování, lze použít funkci hustoty pravděpodobnosti (derivace rozdělovací funkce).

$$P_A = 3 * p - 6 * p^2 + 3 * p^3 \tag{6.41}$$

Pro výpočet je potřeba derivovat funkci č. 6. 41, poté najít lokální extrémy a pak je potřeba zjistit charakter extrémů. Pro počítání všech potřebných údajů budeme používat matematický program MATLAB.

Nejdřív je potřeba udělat derivace prvního řádu funkce č. 6. 41.

```
syms p
PA=3*p-6*p^2+3*p^3;
z=diff(PA);
```

Poté nám vznikne rovnice č. 6. 42

$$P_A = 3 - 12\mathrm{p} + 9 * p^2 \tag{6.42}$$

Dále při pomoci funkce **p1=solve(z);** MATLAB vypočítá kořen rovnice č. 6. 42. Ve výsledku rovnice č. 6. 42 má dva kořeni $p_1 = 1$ a $p_2 = 0{,}33$.

Aby spočítal charaktery extrému je potřeba udělat derivace druhého řádu funkce č. 6. 41.

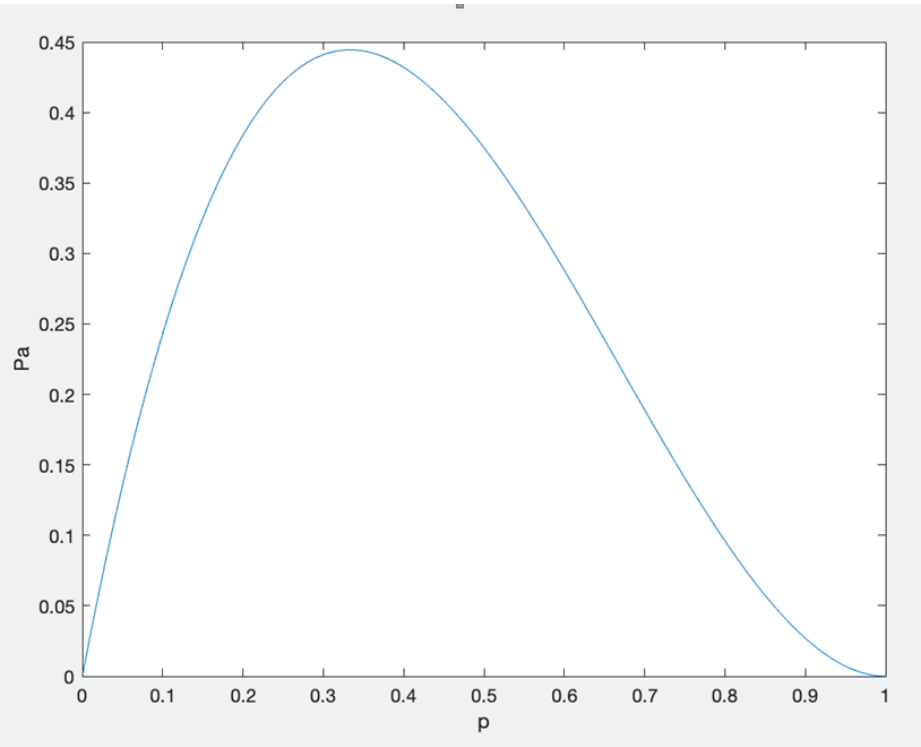
```
q=diff(z);
```

$$P_A = -12 + 18 * \mathrm{p} \tag{6.43}$$

Abychom našli charakter extrému, je potřeba do rovnice č. 43 dosadit kořeny p_1 a p_2, pak vyjde, že při hodnotě $p_2 = 0{,}33$ rovnice. 43 bude se rovnat -6, při $p_1 = 1$ rovnice č. 43 se bude rovnat 6, což podle teorie znamená: pokud je druhá derivace větší než nula, funkce v bodě p je minimum, pokud druhá derivace funkce p je menší než nula, pak je v bodě p maximum funkce. [23]

Ze spočtených údajů můžeme vykreslit graf v závislosti pravděpodobnosti „P_A“ na „p“. Pro vykreslení grafu použijeme aplikaci MATLAB. viz graf č. 1.

```
p = 0:0.01:1;
plot(p,3*p-6*p.^2+3*p.^3);
ylabel('Pa');
xlabel('p');
```



Graf 1: Průběh závislosti P_a na p

Ve druhém případě (nedetekovaní osoby na průchodů P_B) je potřeba stejným způsobem spočítat lokální extrémy a charakter extrémů.

Při počítání bude vycházet z rovnice č. 6. 44.

$$P_B = 3 * p^2 - 3 * p^3 - 1 \tag{6.44}$$

Nejdříve je potřeba udělat z rovnice č. 6. 44. derivace prvního řádu. Pro vypočet budeme používat program MATLAB.

syms p

PA=3*p^2-3*p^3-1;

z=diff(PA);

Poté nám vznikne rovnice č. 6. 42.

$$P_A = 6 * \mathrm{p} - 9 * p^2 \tag{6.45}$$

Dále při pomoci funkce **p1=solve(z);** MATLAB vypočítá kořeny rovnice č. 6. 45. Ve výsledku má rovnice č. 6. 45 dva kořeny p_1 = 0,66 a p_2 =0.

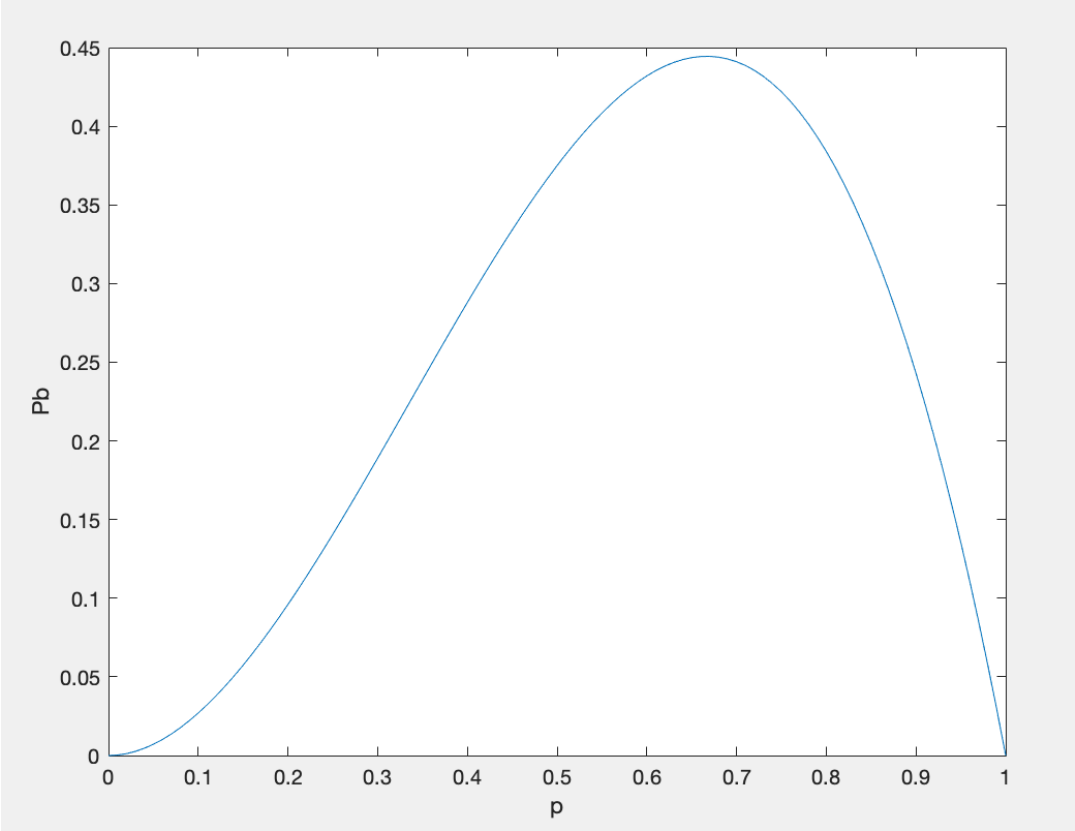
Abychom spočítali charaktery extrému je potřeba udělat derivace druhého řádu funkce č. 6. 44. **q=diff(z);**

$$P_A = 6 - 18 * \mathrm{p} \tag{6.46}$$

Aby se našel charakter extrému je potřeba do rovnice č. 6. 46 dosadit kořeny p_1 a p_2 , pak vyjde, že při hodnotě p_1=0,66 rovince č. 6. 46 se bude rovnat -2, při p_2 = 0 rovnice č. 6. 46 se bude rovnat 2, což podle teorémy znamená: pokud druhá derivace je vetší než nula, funkce v bodě p je minimum, pokud druhá derivace funkce p je menší než nula, pak je v bode p je maximum funkce.

Ze spočtených údajů můžeme vykreslit graf v závislosti pravděpodobnosti „$P_И$“ na „p“. Pro vykreslení grafu použijeme aplikaci MATLAB. viz graf č. 2.

```
p = 0:0.01:1;
plot(p,3*p^2-3*p^3);
ylabel('Pи');
xlabel('p');
```



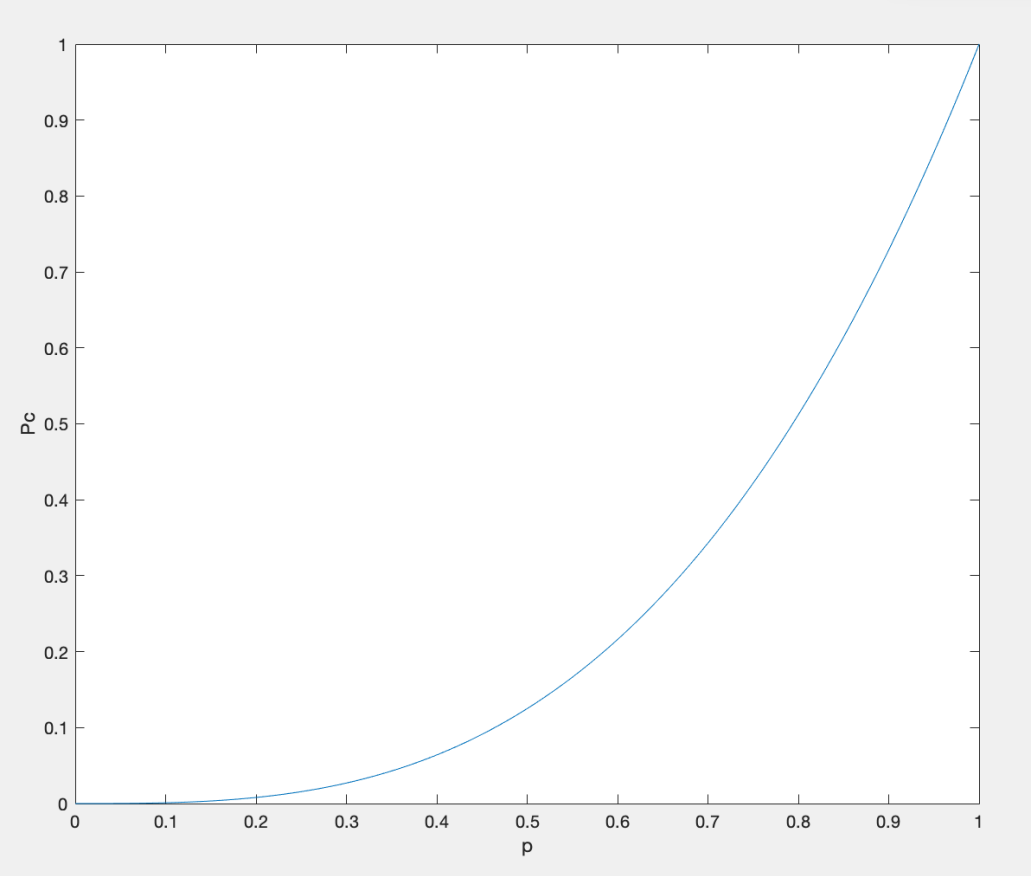
Graf 2: Průběh závislosti P_B na p

Z výsledků je vidět, že průběh závislosti „P_B“ na „p“ je víc vpravo. Pro náš případ to znamená, že pravděpodobnost odhalení neoprávněné osoby je nižší než v prvním případě.

Ve třetím případě funkci P_C můžeme považovat za kvalitu bezpečnostního systému. Protože prostor kritické SRA je poslední prostor kam se může dostat neoprávněná osoba. Pro vykreslení funkce závislosti P_C na p budeme počítat s funkcí č. 6. 47. Pro vykreslení závislosti funkci pravděpodobnosti ve třetím případě, také použijeme matematický nástroj MATLAB viz graf č. 3.

$$P_A = 6 * \mathrm{p} - 9 * p^2 \tag{6.47}$$

```
p = 0:0.01:1;
plot(p,p.^3);
ylabel('Pc');
xlabel('p');
```

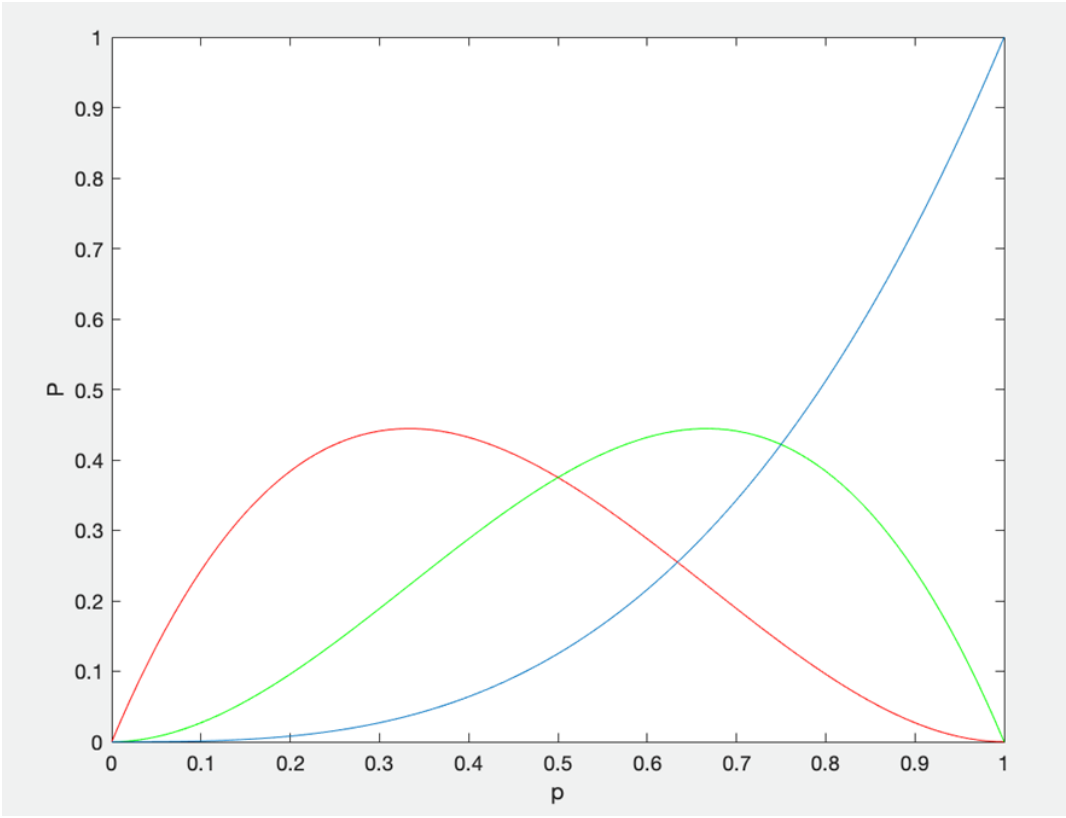


Graf 3: Průběh závislosti Pc na p

Abychom mohli lépe znázornit celkovou pravděpodobnost neodhalení, je vhodné graf č. 1, 2 a 3 sjednotit do jednoho grafu pro přehlednější výsledek. Červená funkce na grafu č. 4 odpovídá funkci pravděpodobnosti neodhalení průchodu neoprávněné osoby mezi veřejným

a neveřejným prostorem, zelená čára na grafu č. 4 odpovídá za funkci pravděpodobností neodhalení při průchodu mezi neveřejným prostorem a SRA prostorem nebo neveřejným prostorem se zvláštním režimovým opatřením. Modrou čarou na grafu č. 4 je označena funkce pravděpodobnosti neodhalení průchodu neoprávněné osoby mezi SRA prostorem nebo neveřejným prostorem se zvláštním režimovým opatřením a kritickým SRA prostorem. Pro vykreslení grafů budeme používat program MATLAB.

```
p=0:0.01:1;
plot(p,3*p-6*p.^2+3*p.^3,'r');
hold on;
plot(p,3*p.^2-3*p.^3,'g');
hold on;
plot(p,p.^3);
 ylabel('P');
xlabel('p');
 hold off;
```



Graf 4: Průběh závislosti P na p

Na grafu č. 4 je znázorněna celková pravděpodobnost detekce na všech třech typech přestupu. Je vidět, že s každým dalším průchodem roste náročnost detekce. A právě klesá pravděpodobnost odhalení při každém dalším průchodů neoprávněné osoby.

7 Návrh aplikace v programu MATLAB.

Z důvodu problematiky bezpečnosti na letišti, která byla zmíněna viz. Kapitola č. 5 a také problematiky ID karet, která je zdůvodněná třemi scénáři: krádež ID karty, ukončení zaměstnaní a kopírování ID karty viz v kapitole č. 4 a také zdůvodněním matematickým modelem pravděpodobnosti nedekování viz kapitola č. 6. se dá říci, že jako samotný systém „ID karta“ pro ověření identity není moc dokonalý, že by bylo lepší používat ID karty spolu se systémem, který by dodatečně mohl ověřit identitu vstupující osoby do neveřejného prostoru letiště. Vzhledem k tomu, že podle Annexu 17 – Bezpečnost, ochrana mezinárodního civilního letectví před protiprávními činy, hlava 3, není přesně určeno, jaká zařízení musí být využita na různých druzích přestupů mezi prostory. [6]

Letiště může navrhnout podle sebe bezpečnostní systém, po schválení Úřadem pro civilní letectví, může být využita bezpečnostní kontrola.

Hlavně po návrhu bezpečnostního systému musí projít schválením úřadu civilního letectví. Ne všechna letiště potřebují mít stejné systémy pro identifikaci zaměstnanců.

Je také velký rozdíl, jak velké je letiště viz kapitola č. 2. Tím pádem by bylo vhodné vytvořit aplikaci, která by za určitých podmínek mohla navrhnout optimální řešení pro aplikace bezpečnostních zařízení systému na určitých typech přestupu.

7.1 Vstupní údaje

Zásadní body pro vypracování modelu, který by navrhnul prvky pro bezpečnostní systém, to jsou parametry, které nám omezí (upřesní) hodnotu výběru.

V modelu používáme rozdělení typu prostoru, o kterém je zmíněno viz kapitola č. 2. To jsou: veřejný prostor, neveřejný prostor, Neveřejný prostor se zvláštním režimovým opatřením, SRA prostor a kritický SRA prostor.

V tabulce č. 5 jsou vidět všechny možné přechody mezi prostory. Podle důležitosti (kritičnosti) prostoru jsou zadány dvě hlavní podmínky, které by měl splnit systém při vyhodnocení nejlepší varianty pro potřebné zařízení na konkrétním přestupu.

První podmínka je požadovaná pravděpodobnost odhalení. Je to hodnota, která definuje bezpečnost (spolehlivost) prvku na konkrétním průchodu. Tato hodnota přímo závisí na typu prostoru. Čím je více potřebné zabezpečit prostor tím je požadovaná pravděpodobnost odhalení vyšší. Tuto hodnu má každé letiště podle potřeby a může si ji nastavit samo podle zařízení, která mají v plánu nainstalovat pro identifikace osob na jednotlivých přechodech.

Druhou podmínkou je jednoduchost přímo spojená s první podmínkou. Protože, čím vyšší je požadovaná pravděpodobnost odhalení, tím je jednoduchost systému nižší. To znamená, že na přestupech s vysokým potřebným bezpečnostním opatřením bude potřeba systém (systémy), který bude odpovídat úrovni spolehlivosti. V tomto případě je jednoduchost systému zanedbatelný faktor.

Pro výpočet jednoduchosti bylo použito zaznamenání průchodu aktérů, kteří mají povolený vstup do neveřejného prostoru letiště Praha. Zaznamenávání se počítalo na průchodů mezi veřejným a neveřejným prostorem na bráně č. 1. viz obrázek č. 14.
Pro vypočet jednoduchosti průchodu mezi veřejným a neveřejným prostorem zaznamenávání průchodu se provádělo ve špičkový čas mezi 7:30-8:30 v pracovní den. Za hodinu bránou č. 1 prošlo 128 osob. Což podle vzorce č. 7.1 odpovídá jednoduchosti zařízení 2,13.

Obrázek 14: Rozmístění brán.

$$jednoduchost\ zařízení\ (propustnost) = \frac{osoba}{minutu} \tag{7.1}$$

Dále pro zjištění jednoduchosti mezi neveřejným prostorem a SRA prostorem bylo zjištěno, že při sledování průchodu aktérů na bráně č. 5., která se nachází, viz obrázek č. 14, bylo zkontrolováno 30 osob. Což podle vzorce č. 48 znamená, že jednoduchost zařízení se rovná 0.5.
Vzhledem k tomu, že nebylo možné zajistit počet pochybujících se osob mezi neveřejným prostorem a neveřejným prostorem se zvláštním režimovým opatřením, budeme počítat s tím, že je potřeba stejná jednoduchost, jako je v případě průchodu mezi neveřejným prostorem a SRA prostorem.
Pro jednoduchost průchodu mezi SRA prostorem a kritickým SRA prostorem budeme používat stejnou jednoduchost jako v případě průchodu mezi neveřejným prostorem a SRA prostorem, protože na letišti v Praze jsou prostory SRA a kritický SRA sloučeny do jednoho prostoru viz tabulka č 5.

Tabulka 5: Požadovaná podmínky.

Typy prostorů	Požadována pravděpodobnost odhalení	Jednoduchost zařízení [osob/minutu]
Veřejný prostor – Neveřejný prostor	0,8	2,13
Neveřejný prostor – Neveřejný prostor se zvláštním režimovým opatřením	0,99	0,5
Neveřejný prostor – SRA prostor	0,99	0,5
Neveřejný prostor se zvláštním režimovým opatřením – Kritický SRA prostor	0,99	0,5
SRA prostor – Kritický SRA prostor	0,99	0,5

Dále je potřeba stanovit seznam a charakteristiku prvků, vzhledem k tomu, že podmínky, podle kterých bude systém hlídat kombinace, jsou požadovaná pravděpodobnost odhalení a jednoduchost zařízení. Při vyhodnocení kombinace prvků programu bude také zohledněna cena této kombinace, protože finanční faktor je důležitým faktorem pro plánování rozpočtu modelování letiště. Cena zařízení je přímo závislá na jednoduchosti prvku. Čím je zařízení levnější, tím je pravděpodobnost odhalení menší.

V tabulce č. 6 jsou znázorněna data, ze kterých jsou namodelovány programy a ze kterých budou vyhodnocovat podle podmínek kombinace bezpečnostních zařízení.

Tabulka 6: Typy zařízení a jejich charakteristiky.

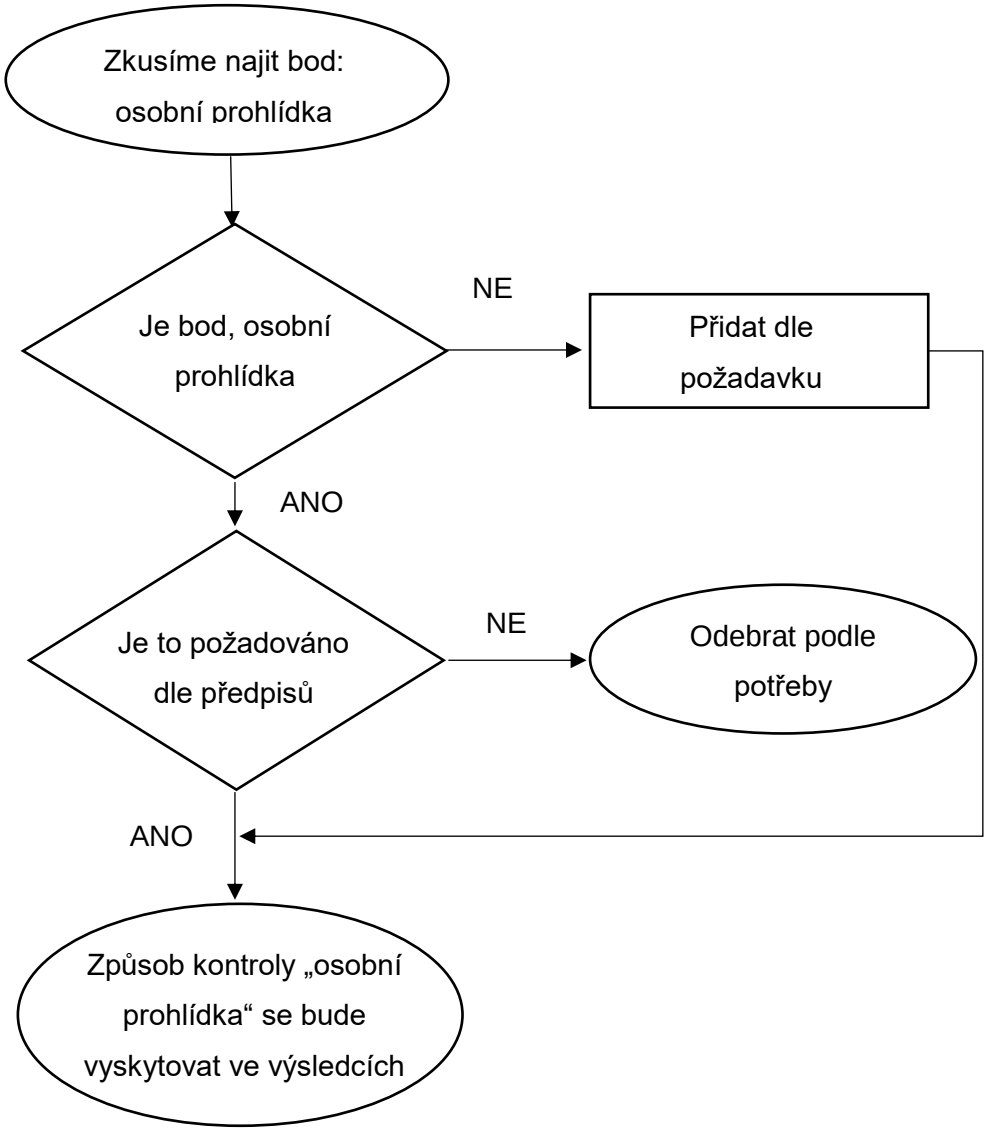
	Typy bezpečnostních zařízení	Požadována pravděpodobnost odhalení	Cena zařízení	Jednoduchost zařízení. Propustnost osoba za minutu
1	Id karta	0,7	500 000,00 CZK	0,12
2	Id karta + kód	0,75	600 000,00 CZK	1,5
3	Id karta + otisk prstu	0,8	800 000,00 CZK	0,5
4	Id karta + geometrie obličeje	0,99	10 000 000,00 CZK	0,3
5	Id karta + hlasová identifikace	0,8	1 200 000,00 CZK	0,4
6	osobni prohlídka	0,98	1 000 000,00 CZK	0,2
7	Systém docházky	0,8	400 000,00 CZK	0,14
8	Systém pro hledání vstupu a výstupu	0,85	700 000,00 CZK	0,14
9	Rentgen/ auto rentgen	0,9	20 000 000,00 CZK	0,3
10	Kamerový systém	0,85	12 000 000,00 CZK	0,01
11	Jednoduchý turniket	0	40 000,00 CZK	2,13
12	Turniket + zařízení s ověřením identity	0,6	657 654,00 CZK	0,5
13	Kamerový systém ve veřejném prostoru	0	20000000,00 CZK	0,2

Všechny charakteristiky (požadována pravděpodobnost odhalení, cena zařízení a jednoduchost zařízení), které jsou uvedeny v tabulce č. 6, nejsou zcela reálná čísla, ale jsou přiblížená k reálným hodnotám. To využita pro znázornění funkčnosti programu.

7.2 Vyhodnocení optimální kombinace zařízení ze vstupních údajů

Jak již bylo zmíněno, program pro vypočítání optimální sestavy zařízení byl naprogramován pomocí programu MATLAB.

Pro modelování bylo použito několik pravidel a podmínek pro zajištění potřebných výsledků. Jednou z těchto podmínek bylo, že na přestupu z neveřejného prostoru nebo z neveřejného prostoru se zvláštním režimovým opatřením do SRA prostoru nebo do kritického SRA prostoru musí byt zařízení č. 6 a 9 viz tabulka č. 6. Podmínka, která musí být splněna v kódu programu funguje na základě blokového diagramu č. 10.



Blokový diagram 11: Programování podmínky.

Další podmínkou a zároveň hlavní podmínkou pro vyhodnocení sestavy zařízení je vyhodit zařízení, která splňují podmínky pro jednotlivý typ přechodu.
Pro výpočet budeme používat De Morganův zákon. De Morganův zákon je logické pravidlo, které spojuje logickou operaci pomocí popření. Tento zákon je vhodně využit, protože vyhodnocujeme zařízení, která musí splňovat dvě podmínky zároveň, ale která jsou vzájemně nezávislá. Pravděpodobnost sjednocení jevů lze využit rovnicí č. 7. 2. [24]

$$P\left(\bigcup_{k=1}^{\infty} E_k\right) = 1 - \prod_{k=1}^{\infty} P(E_k^c) = 1 - \prod_{k=1}^{\infty} \left(1 - P(E_k)\right) \tag{7.2}$$

Po spouštění programu aplikace nám ukáže výsledek viz obrázek č. 15.

```
vyslednaKombinace =

     7     0     0     0     0     0     0     0     0     0     0     0     0
     6     9     0     0     0     0     0     0     0     0     0     0     0
     6     9     0     0     0     0     0     0     0     0     0     0     0
     6     7     0     0     0     0     0     0     0     0     0     0     0
     6     7     0     0     0     0     0     0     0     0     0     0     0


vyslednaCena =

      400000
    21000000
    21000000
     1400000
     1400000
```

Obrázek 15: Výsledná cena. Výsledná kombinace.

Na horní části obrázku č. 15 je znázorněná výsledná kombinace zařízení, které vyhodnotil program. Čísla v prvních dvou sloupcích odpovídají zvoleným typům zařízení ze seznamu, viz tabulka č. 6 (první sloupec). Druhá část odpovídá ceně zařízení, která vyhází z výsledné kombinace. Ve výsledku tyto hodnoty provozovatel letiště může použít pro představu o typu kontroly, kterou může použít na přechodech. Také provozovatel letiště by tak při začátku stádia plánování letiště měl přehled o rozpočtu stavby letiště.

8 Závěr

Cílem této práce bylo znázornit vliv identifikačních karet na celý bezpečnostní systém letiště a dokázat, že je třeba mu věnovat dostatečnou pozornost.

Pro dosažení tohoto cíle bylo potřeba probrat faktory, které ovlivňují danou problematiku. Jedním z těchto faktorů je legislativa civilního letectví (legislativa EU, legislativa ČR) a mezinárodní právní předpisy, které určují minima pro bezpečný provoz. Jeden z hlavních dokumentů, který se zabývá bezpečností v civilní letecké dopravě, je letecký předpis L 17 „Bezpečnost, ochrana mezinárodního civilního letectví před protiprávními činy".

Dalším faktorem této problematiky bylo správné definování typů letiště a typů letištních prostorů. Ještě jedním faktorem, který pomohl dosáhnout cíle, je definování typu narušení. Všechny tyto faktory jsou důležité pro problematiku dané práce a také jsou důležité pro správné modelování bezpečnostního systému letiště.

Model bezpečnostního systému je přesně definován v NBP, také je daná přesná struktura, osnova a také jsou k dispozici základní procesy pro tvorbu bezpečnostního programu letišť.

Další důležitým aspektem pro modelování bezpečnostního systému letiště je správné definování míst zabezpečení a také definování osob, které mají přístup do neveřejných prostorů letiště. Každá osoba, která se pohybuje v neveřejném prostoru letiště, musí mít identifikační kartu na viditelném místě. Výjimku mají jen cestující, kteří nemají identifikační karty. Pro potvrzení potřebné přítomnosti v neveřejném prostoru slouží palubní lístek.

Vzhledem k tomu, že cílem bylo znázornit, jaký vliv mají identifikační karty na bezpečnostní systém letiště, dalším krokem pro dosažení cílů bylo věnování se typům a technickým charakteristikám plastových karet. V této práci byly popsány tři typy plastových karet: reliéfní karty, magnetické karty a smart karty. Při zkoumání těchto typů karet bylo zjištěno, že nejmodernějším a nejspolehlivějším typem karet jsou smart karty.

Vzhledem k technickým charakteristikám plastových karet byly jednoduše definovány výhody a nevýhody plastových karet, které mají vliv na bezpečnostní systém letišť. Podle legislativy a národního bezpečnostního programu musí být identifikační karty součástí bezpečnostního systému letiště. Vzhledem k různým útokům na bezpečnostní systém letiště a útokům na kartový systém se dá jednoduše říct, že kartový systém jako samostatný není dokonalý a je lépe ho využívat společně se systémem, který by mohl dodatečně ověřit identitu.

V historii bezpečnosti letecké dopravy bylo bezpečnostní nastavení zaváděno až po spáchání činu. Celosvětově je bezpečnost letištního systému v současné době na velmi vysoké úrovni. Díky rychlému vývoji technologií je i přesto potřeba neustále aktualizovat bezpečnostní systémy a zamezit dalším teroristickým a jiným činům, jelikož letecká doprava byla a stále je velmi citlivá na možné útoky. Pomoci zdůraznit problematiku této práce pomohla analýza

všech možných scénářů. Co všechno se mohlo stát při krádeži nebo ztrátě ID karty, ukončení zaměstnaní nebo kopírování ID karty. Tyto tři scénáře jsou znázorněny pomocí blokových diagramů a každý scénář byl znázorněn na každém možném typu přechodu. Typy přechodů definují jednotlivá místa na letiště, na kterých je prováděna kontrola totožnosti zaměstnanců. Typy přechodů rozumíme přechod mezi veřejným a neveřejným prostorem, přechod mezi neveřejným prostorem a SRA prostorem nebo prostorem se zvláštním režimovým opatřením anebo přechod mezi SRA prostorem nebo neveřejným prostorem se zvláštním režimovým opatřením a kritickým SRA prostorem.

Po zkoumání všech typů scénářů a problémů s tím spojených byl vytvořen matematický model detekce pohybu neoprávněné osoby mezi neveřejnými prostory. Tento model na základě počítání pravděpodobnosti při průchodu neoprávněné osoby mezi neveřejnými prostory dokázal to, že při každém dalším průchodu pravděpodobnost odhalení neoprávněné osoby se snižuje. To znamená, že nejvyšší pravděpodobnost odhalení je mezi přechodem z veřejného do neveřejného prostoru. Výsledek ze spočítané pravděpodobnosti ukazuje, že by bylo lepší využívat ID kartu společně s doplňkovým systémem ověření identity už na prvním přechodu.

Pro plánování bezpečnostního systému letiště je potřeba správně určit zaměření letiště a jaký bude mít letiště provoz. Z těchto faktorů je možné jednoduše namodelovat soustavu systémů bezpečnostních zařízení na jednotlivé typy přestupu. Z tohoto důvodu byl vytvořen program přes aplikaci MATLAB, který při zadání určitých podmínek (požadovaná pravděpodobnost odhalení a jednoduchost zařízení) pomůže jednoduše navrhnout umístění bezpečnostních zařízení pro konkrétní přechod.

Při programování tohoto systému byla využita data zaznamenávaná při průchodu zaměstnanců na letiště v Praze přes veřejný a neveřejný prostor a také přechod mezi neveřejným prostorem a SRA prostorem. Namodelovaný program vyhodnocuje výsledky z požadovaných podmínek uživatelů. Výsledek je představen kombinací čísel, který odpovídá konkrétním zařízením ze zvoleného seznamu.

V návaznosti na veškerou řešenou problematiku v práci je možné stanovit, že cíl práce byl splněn.

Bibliografie

[1] B. Koverdynský, Historie, organizace, standarty a postupy, Cheb: Svět křídel, 2014.

[2] Úřad pro publikace Evropské unie, „Evropská rada: padesát let evropských summitů," 12 2011. [Online]. Available: https://www.consilium.europa.eu/media/31015/qc3111406csc.pdf.

[3] Úřad pro civilní letectví, „EU legislativa," [Online]. Available: http://www.caa.cz/ochrana-civilniho-letectvi/eu-legislativa. [Přístup získán 20 4 2019].

[4] Ústav letecké dopravy Fakulta dopravní ČVUT v Praze, *Metodika pro tvorbu bezpečnostních programů mezinárodních letišť,* Praha: Ústav letecké dopravy Fakulta dopravní ČVUT v Praze.

[5] Ministerstvo dopravy Českérepubliky,, *Zákon č. 49/1997 Sb., o civilním letectví,* Praha: Ministerstvo dopravy České republiky, 1997.

[6] Úřad pro civilní letectví. Letecká informační služba. L-17 Bezpečnost, ochrana mezinárodního civilního letectví pře protiprávními činy, „Letecká informační služba," [Online]. Available: http://lis.rlp.cz/predpisy/predpisy/index.htm. [Přístup získán 15 3 2019].

[7] Úřad pro civilní letectví. Národní bezpečnostní program., „Úřad pro civilní letectví," [Online]. Available: http://www.caa.cz/ochrana-civilniho-letectvi/nbp-narodni-bezpecnostni-program.

[8] Úřad pro civilní letectví. Národní program bezpečnostního výcviku, [Online]. Available: http://www.caa.cz/ochrana-civilniho-letectvi/narodni-programy.

[9] Úřad pro civilní letectví. Národní program řízení kvality bezpečnostních opatření k ochraně civilního letectví České republiky před protiprávními činy, [Online]. Available: http://www.caa.cz/ochrana-civilniho-letectvi/narodni-programy.

[10] V. Zharkova, *Bakalářská práce. Incentivní programy na mezinárodních letištích,* Praha: České vysoké učení technické v Praze, 2016.

[12] P. Michaela, „Pravidla pro vstup osob a vjezd vozidel a pro jejich pobyt v neveřejném prostoru letiště Praha/Ruzyně," 21 11 2017. [Online]. Available: https://www.prg.aero/sites/default/files/obsah/B2B/Files/Nonaviation%20business/Pro%20obchodni%20partnery/Normy/Bezpecnost/Pravidla%20pro%20vstup%20osob%20a%20vjezd%20vozidel%20a%20pro%20jejich%20pobyt%20v%20neve%C5%99ejn%C3%A9m%20prostoru%20LKPR.pdf. [Přístup získán 24 4 2019].

[13] I. V. Ř. PhD., „Bezpečnostní kontrola při odbavení,“ 1 1 2017. [Online]. Available: https://www.prg.aero/vstupni-rad. [Přístup získán 25 4 2019].

[14] L. Strnad, Bakalářská práce. Vydávání a používání platebních karet, Vysoká škola regionálního rozvoje a Bankovní institut, 2013.

[15] W. Rankl a W. Effing, Smart CardHandbook, Munich, Germany: Carl Hanser Verlag, Munich/FRG, 2003.

[16] I. Turaev, Plastikovyye karty: proiskhozhdeniye, naznacheniye, funktsii, preimushchestva, nedostatki, Moskva, 2010.

[17] G. Selimis, A. Fournaris, G. Kostopoulos a O. Koufopavlou, „Software and Hardware Issues in Smart Card Technology,“ 2009. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5208738.

[18] Wikipedia, „Identifikatsionnyye karty,“ [Online]. Available: https://ru.wikipedia.org/wiki/%D0%98%D0%B4%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5_%D0%BA%D0%B0%D1%80%D1%82%D1%8B.

[19] U. o. Maryland, „Global Terrorism Database,“ 5 2018. [Online]. Available: https://www.start.umd.edu/gtd/. [Přístup získán 5 5 2019].

[20] D. Welch, „ABC news.Airport security card company reveals data hack as AFP investigates,“ 11 7 2018. [Online]. Available: https://www.abc.net.au/news/2018-07-12/afp-investigating-airport-security-card-data-hack/9981796.

[21] L. Letňany, „Bezpečnost na Letišti Praha Letňany,“ 23 11 2015. [Online]. Available: http://www.letnany-airport.cz/?p=1535&lang=cs.

[22] Wikipedia, „Trigonometricheskaya formula Viyeta,“ 2018. [Online]. Available: https://ru.wikipedia.org/wiki/%D0%A2%D1%80%D0%B8%D0%B3%D0%BE%D0%BD%D0%BE%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D1%84%D0%BE%D1%80%D0%BC%D1%83%D0%BB%D0%B0_%D0%92%D0%B8%D0%B5%D1%82%D0%B0.

[23] Kontromat, „Nakhozhdeniye maksimuma i minimuma funktsii odnoy peremennoy.,“ [Online]. Available: http://kontromat.ru/?page_id=888.

[24] P. Lukeš, Bakalářská práce. Pokročilé aspekty modelování zatížení RF pásma 1030/1090 MHz., Praha, 2017.

Seznam diagramů

Seznam tabulek

Seznam obrázků

Seznam blokových diagramů