

# **Možnosti zabezpečení učitelů a studentů před teroristickými útoky v budově U5 na UTB ve Zlíně**

Bc. Nikola Čajková

---

Diplomová práce  
2019



Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky

---

## ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	Bc. Nikola Čajková
Osobní číslo:	A18436
Studijní program:	N3902 Inženýrská informatika
Studijní obor:	Bezpečnostní technologie, systémy a management
Forma studia:	kombinovaná
Téma práce:	Možnosti zabezpečení učitelů a studentů před teroristickými útoky v budově U5 na UTB ve Zlíně
Téma anglicky:	Teachers and Students Security Possibilities Against Terrorist Attacks on the U5 Building at TBU in Zlin

### Zásady pro vypracování:

1. Stručně popište problematiku terorismu a ochrany měkkých cílů.
2. Vyjmenujte a vysvětlete základní terminologii ochrany měkkých cílů a s tím spojenou legislativu.
3. Charakterizujte umístění budovy U5 a posuďte lokalitu, ve které se nachází.
4. Provedte analýzu rizik se zaměřením na násilné útoky.
5. Navrhněte vhodná bezpečnostní opatření.

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. BRZYBOHATÝ, Marian. Terorismus I. vyd. Praha: Vydavatelství POLICIE HISTORY, 1999. ISBN 80-902670-1-7.
2. KALVACH, Z. Základy ochrany měkkých cílů metodika. Vyd.1. Praha, 2016.
3. KYNCL, Jaromír. Bezpečnost objektu ve světle moderních technologií. Praha: Komora podniků komerční bezpečnosti České republiky, 2014. ISBN 978-80-260-7115-0.
4. LUKÁŠ, Luděk et al. Bezpečnostní technologie, systémy a management II. 1. vyd. Zlín: VeRBuM, 2012, 386 s. ISBN 978-80-87500-19-4.
5. LUKÁŠ, L. Bezpečnostní technologie, systémy a management III. 1. vyd. Zlín: VeRBuM, 2013, 456 s. ISBN 978-80-87500-35-4.
6. MAREŠ, Miroslav. Terorismus v ČR. Brno: Centrum strategických studií, 2005. ISBN 80-90-3333-8-9.

Vedoucí diplomové práce:

**doc. Ing. Libor Pekař, Ph.D.**

Ústav automatizace a řídicí techniky

Konzultant:

**Ing. Dora Lapková, Ph.D.**

Ústav bezpečnostního inženýrství

Datum zadání diplomové práce:

**30. listopadu 2018**

Termín odevzdání diplomové práce:

**17. května 2019**

Ve Zlíně dne 14. prosince 2018

doc. Mgr. Milan Adámek, Ph.D.  
*děkan*



doc. RNDr. Vojtěch Křesálek, CSc.  
*ředitel ústavu*

## **Prohlašuji, že**

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

## **Prohlašuji,**

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

Ve Zlíně, dne 11.05.2019

Nikola Čajková, v.r.  
podpis diplomanta

## **ABSTRAKT**

Tato diplomová práce se zabývá návrhem strategie a bezpečnostních opatření proti teroristickým útokům v budově U5, která spadá pod Univerzitu Tomáše Bati ve Zlíně. V teoretické části jsou na základě pohledů různých odborníků a zdrojů definovány a formulovány pojmy a přístupy související se samotným tématem terorismu, dále je osvětlena historie a forma tohoto fenoménu ve světě i na území České republiky a na závěr je pomocí jednotlivých analýz navržen směr pro následující praktickou část. Praktická část v úvodu prezentuje budovu fakulty a následně aplikuje vybrané metodiky analýzy rizik, na jejichž základě jsou vytvořeny konečné návrhy a doporučení pro nápravu současného stavu zabezpečení referenčního objektu.

**Klíčová slova:** Terorismus, teroristický útok, měkké cíle, Univerzita Tomáše Bati, Fakulta aplikované informatiky, FMEA, ETA, analýza rizik

## **ABSTRACT**

This master thesis deals with the design of strategy and security measures against terrorist attacks in the U5 building, which belongs to the Tomas Bata University in Zlín. In the theoretical part, the concepts and approaches related to the very topic of terrorism are defined and formulated based on the views of different experts and sources. The practical part introduces the faculty building and applies selected risk analysis methodologies on the basis of selected final proposals and recommendations for solving the current state of reference object security.

**Keywords:** Terrorism, Terrorist Attack, Soft Targets, Tomas Bata University, Faculty of Applied Informatics, FMEA, ETA, Risk Analysis

## **PODĚKOVÁNÍ**

Tímto bych chtěla poděkovat všem zaměstnancům Fakulty aplikované informatiky, kteří se po celou dobu mého studia podíleli na přátelské atmosféře, která na fakultě panuje, díky kterým mé četné výjezdy do zahraničí byly snadnější a návraty plynulejší.

Dále mé velké poděkování patří panu doc. Ing. Martinu Hromadovi, Ph.D., jehož cenné rady a zkušenosti jsem využila při zpracování této diplomové práce, a také panu doc. Ing. Liborovi Pekařovi, Ph.D. spolu s paní Ing. Dorou Lapkovou, Ph.D. za jejich odborné vedení a nadhled.

V neposlední řadě bych chtěla poděkovat své rodině, která mi je oporou a svým přátelům, jmenovitě Thomas Orak, Zuzana Váňová, Daniel Berger, Daniel Réda a Rui Cristóvão, bez nichž bych nebyla ve fázi psaní těchto řádků. Děkuji.

„Každý člověk na zemi bez ohledu na to, co dělá, hraje vždy hlavní roli v historii světa.

A obvykle o tom neví.“

*Paulo Coelho*

# OBSAH

<b>ÚVOD</b> .....	<b>8</b>
<b>I TEORETICKÁ ČÁST</b> .....	<b>9</b>
<b>1 TERORISMUS</b> .....	<b>10</b>
1.1 HISTORIE TERORISMU .....	10
1.2 ZÁKLADNÍ TYPOLOGIE TERORISMU .....	13
1.3 METODY TERORISTICKÝCH ÚTOKŮ.....	15
1.4 FÁZE TERORISTICKÉHO ÚTOKU.....	17
1.5 MAPOVÁNÍ TERORISMU .....	19
1.6 VÝZNAMNÉ TERORISTICKÉ ÚTOKY .....	21
1.7 TERORISMUS V ČESKÉ REPUBLICE.....	23
1.8 TERORISTICKÉ ORGANIZACE .....	24
1.9 BOJ PROTI TERORISMU.....	27
<b>2 MĚKKÉ CÍLE</b> .....	<b>29</b>
2.1 TERMINOLOGIE Z OBLASTI BEZPEČNOSTNÍ POLITIKY MĚKKÝCH CÍLŮ.....	30
2.2 ÚTOKY NA MĚKKÉ CÍLE V ČR.....	32
2.3 DOSAVADNÍ AKTIVITY PRO OCHRANU MĚKKÝCH CÍLŮ V ČR.....	33
<b>3 ANALÝZA RIZIK</b> .....	<b>35</b>
3.1 VŠEOBECNÉ PŘÍSTUPY K OBSAHU ANALÝZY RIZIK .....	36
3.2 METODY ANALÝZY RIZIK .....	38
3.2.1 Vybrané základní metody analýzy rizik.....	39
3.2.2 Indexové metody .....	43
3.3 BEZPEČNOSTNÍ OPATŘENÍ PRO MINIMALIZOVÁNÍ RIZIK .....	44
<b>II PRAKTICKÁ ČÁST</b> .....	<b>47</b>
<b>4 FAKULTA APLIKOVANÉ INFORMATIKY UTB</b> .....	<b>48</b>
4.1 LOKACE A OKOLÍ OBJEKTU .....	48
4.2 KRIMINALITA .....	50
4.3 SLOŽKY INTEGROVANÉHO ZÁCHRANNÉHO SYSTÉMU .....	52
4.4 POPIS REFERENČNÍHO OBJEKTU .....	53
4.5 PROCESY OBJEKTU .....	57
4.6 IDENTIFIKACE AKTIV .....	62
4.7 NÁVŠTĚVNOST REFERENČNÍHO OBJEKTU .....	64
4.8 BEZPEČNOSTNÍ OPATŘENÍ .....	65
<b>5 FMEA ANALÝZA</b> .....	<b>69</b>
<b>6 ETA ANALÝZA</b> .....	<b>75</b>
<b>7 METODA ANALÝZY RIZIK A HROZEB MĚKKÝCH CÍLŮ</b> .....	<b>83</b>
<b>ZÁVĚR</b> .....	<b>94</b>
<b>SEZNAM POUŽITÉ LITERATURY</b> .....	<b>95</b>
<b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK</b> .....	<b>101</b>
<b>SEZNAM OBRÁZKŮ</b> .....	<b>103</b>
<b>SEZNAM TABULEK</b> .....	<b>105</b>

<b>SEZNAM PŘÍLOH.....</b>	<b>106</b>
<b>PŘÍLOHA P I: ETA ANALÝZY NÁPRAVNÉHO OPATŘENÍ.....</b>	<b>107</b>
<b>PŘÍLOHA P II: VÝPOČTY OHROŽENÍ V ZÁVISLOSTI NA LOKALIZACI A NAČASOVÁNÍ ÚTOKU .....</b>	<b>111</b>



## ÚVOD

Terorismus. Lidmi tolik skloňovaný pojem, který v dnešní době dokázal pevně zakotvit do každodenního slovníku mnohých z nás. Slovo, které spolu s vlnou populismu pomáhá na dnešní politické scéně vyhrávat volby. Slovo, které v lidech dokáže vyvolat různé pocity, ale ve většině převládá jedno – strach. Právě tato slova byla klíčovými při výběru diplomové práce, která se zabývá analýzou rizik s návrhy nápravných opatření objektu, který je pro autorku významný a jehož prostory jsou ji velmi dobře známy. Cílem diplomové práce je tedy navrhnout bezpečnostní opatření, která by pomohla snížit riziko dopadu teroristického útoku na daný referenční objekt.

Teoretická část práce se bude snažit o přiblížení fenoménu terorismu čtenářům. V posloupnosti pojedná o historii vzniku terorismu, popíše rozdělení základní typologie a metod, k jakým se teroristé uchylují při páchání útoku. Pomocí grafického znázornění se pokusí přiblížit jednotlivé fáze násilného útoku a dále promítnout významné teroristické útoky ve světě. V návaznosti na nejtragičtější útoky práce pojedná o nynější situaci okolo terorismu na území České republiky.

V úzké souvislosti s terorismem je v dnešní době značně diskutovaná ochrana měkkých cílů, jejíž terminologií, zaznamenanými útoky a současnou celostátní ochranou se bude zabývat druhá kapitola. Po nastínění problematiky měkkých cílů a důvodu, proč by se na jejich ochranu měl klást větší důraz, se práce bude soustředit na možnosti, jak ke konkrétním objektům, představujícím měkký cíl přistupovat, jak hodnotit a analyzovat míru ohrožení a hlavně, jaké konkrétní metodiky jsou pro daný subjekt vhodné.

Praktická část v začátku seznámí čtenáře se samotným objektem Fakulty aplikované informatiky, jeho dislokací a stručným popisem budov spadajících do jeho blízkého okolí. V návaznosti na dílčí charakteristiku objektu budou pomocí vybraných metodik analyzovány konkrétní potencionální bezpečnostní hrozby, po jejichž ohodnocení budou navržena vhodná bezpečnostní opatření.

## **I. TEORETICKÁ ČÁST**

## 1 TERORISMUS

Definice terorismu není jednotná a pohledy na něj se v mnoha ohledech očí různých odborníků liší. Traduje se, že bylo sepsáno tolik slov na téma definice terorismu, jako bylo tímto násilným útokem prolito kapek krve. Pouze dvojice Alex P. Schmid a Albert J. Jongman ve své knize uvedla přes sto různých druhů definování terorismu. [1]

Jednou z definic terorismu je: „Jedná se o metodu či způsob použití síly nebo hrozby silou s cílem vyvolat takové psychologické účinky (strach), které povedou k dosažení určitých, zejména politických cílů“. [2] K uznávaným definicím terorismu také patří definice podle prof. JUDr. PhDr. Miroslava Mareše, Ph.D.: „Terorismus je použití agresivního a excesivního násilí (anebo hrozba použitím takového násilí), které je naplánováno s dominantním účelem vyslat vážené zastrašující poselství zřetelně většímu počtu lidí (cílovému publiku) než pouze těm, kteří jsou primárními násilnými akty nebo hrozbami bezprostředně poškozeni.“ [3]

Ať už se jednotlivé definice liší jakkoliv, kořen slova „terror“ je odvozen z latinského slova „terrere“ a znamená vyděsit či zastrašovat [4], což popisuje emoce, které nastávají při každém teroristickém útoku, kdy strach pojímá množství lidí, včetně těch, kteří konkrétním teroristickým útokem osobně postiženi nemuseli být.

Do podvědomí široké veřejnosti se terorismus dostal při útoku ve Spojených státech amerických, kdy v den 11. září 2001 přišly tisíce nevinných občanů o život a nespočetné množství dalších nevinných utrpělo újmy fyzického, a především psychického charakteru. [5]

Od tohoto pomyslného milníku se setkáváme a doslýcháme o teroristických útocích každoročně po celém světě. Většina těchto útoků je promyšlených, dlouhodobě plánovaných a jsou páchany z nejrůznějších důvodů. Je velmi těžké tyto útoky včas odhalit a zabránit jim především, pokud jsou zaměřeny proti bezbranným občanům, rozhození infrastruktury, vytvoření chaosu a strachu. Ve snaze většiny dnešních států je proto zdokonalit preventivní bezpečnostní opatření pro obranu proti možnému teroristickému útoku.

### 1.1 Historie terorismu

Terorismus je součástí lidstva od prvopočátků existence. Již ve starém Řecku a Římě se prováděly atentáty nejrůznějších typů na vysoce postavené představitele a vůdce. Užívání terorismu jako pojmu začalo v době Velké francouzské revoluce, tedy v 18. století, kdy se takto označovala vláda spojená s tyraníí a vláda, založena na hrozbě násilím. „V době Velké

francouzské revoluce se terorismus paradoxně objevuje v pozitivním znění, kdy podle jeho vykonavatelů je symbolem ctnosti a demokracie. Byl využit při vynucování pořádku ze strany státní moci proti anarchistickým buřičům, jenž se snažili povstáním a nepokoji o zhroucení vlády. Naopak proti této tezi, že terorismus je vlastně pozitivní věc, se v 19. století vžil pojem, že terorismus je hlavním nástrojem sociálních revolucionářů, kteří pořádají atentáty na osoby z řad vládnoucí třídy“. [6]

Přesto, že podstata terorismu se více či méně nezměnila, charakter a samotné provedení násilného činu od dob Velké francouzské revoluce prošlo značným vývojem. Nejen že za propracovanými technikami a fázemi útoku moderní doby stojí vývoj lidstva jako takového, ale velkou roli sehrává také technologický pokrok. Dle Mgr. et Mgr. Ondřeje Filipce, Ph.D. lze vývoj terorismu rozdělit na čtyři jednotlivé éry, založené na rozdílnosti uchopení faktorů v dané době, jakými jsou například financování, cíle útoku, kvalita vykonaného útoku a forma organizace. [7] Jednotlivými érami jsou:

- Primitivní terorismus

Období primitivního terorismu zaznamenává dobu od počátků lidstva a s tím spojené první útoky, které ve své pravé podstatě symbolizovaly stejný záměr, jako záměr novodobých teroristů. Útočníci při útoku využívali jednoduchých metod a zbraní, ke kterým patřily zejména chladné zbraně – dýky, kopí, biče, bodce. Dále byly častou volbou v páchání zločinů za pomoci ohně a jedů, při jejichž použití bylo zapotřebí plánování metody útoku. Typickým příkladem primitivního terorismu je zavražděný římský vojevůdce Gaius Julius Caesar a římský císař Gaius Caesar Augustus Germanicus. V obou případech došlo k útoku rozhněvaným davem, který po předchozím uvážení zvolené metody usmrtil oběť chladnou zbraní. [7, 8]

- Pokročilý terorismus

Oproti primitivnímu terorismu využívá při útoku zbraně, fungující na principu střelného prachu a jednoduchých výbušnin. Pokročilý terorismus vzhledem k rozdílnosti vývoje jednotlivých zemí nemá přesné časové hranice. Hlavním symbolem tohoto období je střelný prach, který po vynalezení (Čína) zásadně změnil dosavadní způsoby útoků a po jeho rozšíření nastala revoluce i ve vojenském sektoru. [9]

Dalším výrazným prvkem tohoto období byl dynamit, který se původně využíval v těžebním průmyslu, odkud se ilegálně dostával do rukou útočníkům a následně byl zpracován teroristickými skupinami. Příkladný útok zastupující tuto éru je tzv. dynamitová válka, ve které

skupina Irských teroristů v osmdesátých letech 19. století usilující o prosazení republikánského zřízení v Irsku zaútočila velkým množstvím dynamitu na měkké cíle – radnice, vlaková nádraží, vlakové tratě a banky ve městech Manchester, Liverpool a Londýn. [10]

- Moderní terorismus

Éra moderního terorismu spadá do druhé poloviny 20. století, pojí se s obdobím studené války a je pro ni typický rozvoj terorismu. Objevují se nové metody a prvky pro posílení terorismu jako například únosy letadel, financování státních aktérů, využívá se velkého vlivu médií a komunikační technologie se dostávají na mezinárodní úroveň, což teroristickým skupinám otevírá nové možnosti. [7]

Mimo jiné se do teroristických skupin v této éře dostávají k činu také ženy, které přinesly fenomén s propojením sebevražedného terorismu. Typický příklad se stal 21. května roku 1991 [11], kdy tamilská atentátnice zaútočila na indického politika se 700 g trhaviny hexogenu a Rádžív Gandhí umřel spolu se 14 lidmi v blízkém okolí. Ženská síla byla využívána v rámci druhé světové války, ve které se prolomily pomyslné ledy v rozdílnosti mezi mužem a ženou, a proto po skončení války pro mnoho žen vkročit do teroristických skupin nebyla otázka. Libanon roku 1985 zaznamenal útok několika žen v automobilech s trhavinami, které najely do izraelských vojáků a spáchaly útok, naloženými trhavinami. [12]

- Postmoderní terorismus

Postmoderní terorismus je charakteristický profesionalitou a propracovaností útoků teroristů. Typickými mezníky této éry je útok na konci dvacátého století v Tokiu, kdy skupina útočnicků vyrobila bombu, obsahující látku, která paralyzovala zasaženým osobám nervovou soustavu. Tento čin patří k mezním hlavně proto, že byla paralyzující látka vytvořena samotnými teroristy a její odpálení proběhlo v prostorách metra – měkký cíl – a bylo tedy zasaženo mnoho nevinných osob. [13]

K dalším mezníkům této éry patří událost z 11. září 2001, která proběhla ve Spojených státech. Tento útok v sobě odráží dokonalou organizaci personálních složek, precizní načasování jednotlivých kroků útoku, odbornost jednotlivých útočnicků a v neposlední řadě využití hromadného civilního prostředku, jehož výstup je srovnatelný či přesahující s využitím armádního prostředku. Éra postmoderního terorismu se vyznačuje využitím veškerých prostředků a znalostí pro posílení moci, jakými jsou například informační technologie, kyber-

netika a globální síť. Specifické rozdílnosti mezi tradičním (primitivní a pokročilý) a novodobým (moderní a postmoderní) terorismem, jsou popsány v níže přiložené tabulce (Tab. 1). [5, 7]

Tab. 1: Rozdíly mezi novodobým a tradičním terorismem [7]

	<b>Tradiční terorismus</b>	<b>Novodobý terorismus</b>
<b>Organizace</b>	Určitelná	Méně určitelná
<b>Forma organizace</b>	Zpravidla hierarchická	Spíše lineární
<b>Operační kvalita</b>	Střední profesionalizace	Plná profesionalizace
<b>Síla skupiny a rekruční potenciál</b>	Malá až střední síla, omezený rekruční potenciál	Individuum nebo malá skupina, vysoký rekruční potenciál
<b>Operační území</b>	Regionální nebo národní	Mezinárodní
<b>Operační cíle</b>	Předvídatelné a identifikovatelné	Špatně předvídatelné a špatně identifikovatelné
<b>Oběti a jejich počet</b>	Vybrané, malé počty	I nevybrané s možností velkého počtu
<b>Kvantitativní rozměr hrozby</b>	Omezený vztah k efektu a následkům	Vzrůstající vztah k efektu a následkům
<b>Intelektuální motivace k veřejnému přihlášení</b>	Vysoká	Ubývající
<b>Spojení s organizovanou kriminalitou</b>	Relativně malé	Intenzivní
<b>Možnosti financování</b>	Malé (závislé na únosech, loupežích a vydírání)	Velké (přístup k mezinárodním zdrojům)

## 1.2 Základní typologie terorismu

Terorismus se dělí do jednotlivých typologií na základě motivace útočníků k vykonání teroristického útoku, zaměření na specifické cíle nebo použití různých prostředků. Třídění motivace terorismu je obdobně složité, jako nalezení jeho přesné definice, jelikož se jednotlivé motivace pro uskutečnění teroristického útoku mohou libovolně překrývat a prolínat s různou mírou intenzity. Jednotlivá rozdělení terorismu jsou stručně popsána v této podkapitole.

- Ultralevicový

„Pojem krajní levice (ultralevice) označuje část politického spektra, která je charakteristická vyhraněným zdůrazňováním egalitářství<sup>1</sup>. Tento atribut je většinou doplněn o akční a razantní metody prosazování zájmů“. [3]

Ve své podstatě je ideologie krajní levice opřena o tvorbu Bedřicha Engelse a Karla Marxe a můžeme ji rozdělit na dva ideologické proudy – komunismus a anarchismus. Jednotlivé skupiny ultralevicového terorismu se mohou od této ideologie mírně odklánět. Anarchistické skupiny teroristů byly zaznamenány hlavně na území Evropy. V České republice se k zástupcům ultralevicového terorismu anarchistů řadí skupiny Anarchistického černého kříže a Antifa. [14]

- Ultrapravicový

Krajně pravicový terorismus nejvíce zasáhl naše dějiny v období druhé světové války. Nacistické a fašistické ideologie jsou nyní následovány ve formě nově vzniklých extremistických skupin, ve kterých hraje velkou roli antisemitismus s xenofobií. Tento extremistický směr je zacílen na politickou stránku země, kdy se snaží v dané zemi zničit panující demokracii a poté postupným oslabením převzít moc státu. [3]

- Etnický a teritoriální

Etnický terorismus klade důraz na zájmy daného etnika, zatímco teritoriální terorismus je zaměřen hlavně na zájem o statut daného teritoria. V praxi však nezřídka dochází k prolnutí obou směrů. Ve své podstatě jde aktivistům zejména o založení nového státu pro lid se specifickým etnikem. [3]

Rozkvět tohoto terorismu panoval v období po druhé světové válce, kdy se vytvořené kolonie měly tendence osamostatnit a vytvořit zcela nový stát, jako tomu bylo v případě Kypru a Alžírsku. [15]

---

<sup>1</sup> Egalitářství je víra, která klade důraz na lidskou rovnost. V rámci víry prosazuje veškeré donucovací prostředky pro udržení plošné rovnosti, s níž se údajně lidé narodí. [16]

- Náboženský

Tento druh terorismu se soustředí na prosazování ideologií vytyčeného náboženství a uplatňuje zákony daného státu k jeho prosazování. Velké zastoupení náboženského terorismu pochází z islámských států, kde se jednotliví členové teroristických organizací vyznačují až nepochopitelným fanatismem. Do rukou islámské organizace Al-Kaida spadá i nejtragičtější teroristický útok z data 11. září 2001, který měl za následek bezmála tři tisíce obětí. K jednoznačným zástupcům v Evropě patří Irsko, které již několik let sužuje svým separatickým a nacionálním zaměřením. [5]

- Ekologický

Ekoterorismus se začal objevovat okolo sedmdesátých let v závislosti na vyšším povědomí veřejnosti v této problematice, což postupně začalo ovlivňovat i politickou a ekonomickou sféru. Aktivisty ekologického terorismu nebo také ekoterorismu, můžeme rozdělit do dvou skupin. Jedna skupina ekoterorismů uplatňuje veškeré síly pro ochranu životního prostředí na naší planetě, práva zvířat, kácení lesů apod. Na druhou stranu se řadí členové, uplatňující teroristické metody proti těmto skupinám, ve snaze poškodit životní prostředí. K této straně se často připojují i skupiny krajně levicových organizací. [1]

- Jednopoložkový

Jednopoložkový typ terorismu nebo také Single-issue terorismus je extremistické chování jednotlivců nebo skupin, kteří protestují a projevují své názory obvykle ve spojení s vládní nečinností. Obecně se tento druh terorismu pojí s tematikou práv zvířat, životního prostředí a potratů. [17]

### 1.3 Metody teroristických útoků

Vědomě spáchaný násilný čin si žádá v mnoha případech dlouhodobé plánování. V rámci plánování je zapotřebí vhodná volba metody uskutečnění teroristického útoku, která ve výsledku koresponduje s myšlenkou provedení a zanechá správnou „message“. Jednotlivé metody se od sebe odlišují nejen v provedení, ale i v účinnosti, následcích a rozlohou působení zvolené metody.

- Tradiční

Jako jednoduchá metoda násilného teroristického útoku se řadí založení požáru. Žhářství patřilo mezi časté útoky v éře primitivního terorismu a dodnes se řadí mezi účinné formy



ataku, kdy veškeré prostředky k provedení jsou lehké k obstarání a výsledek s sebou může nést nejen újmy na životech, ale také škodu na majetku v závislosti na rozloze požáru. U žhářství velmi záleží na době a lokaci provedeného útoku.

K dalším metodám teroristického útoku spadá útok střelnou zbraní. Od dob primitivního terorismu se z luků a šípů zbraně vyvinuly do forem například útočných pušek M16, které i samy o sobě prošly od roku 1963 radikálním vývojem po například špičkové německé kompaktní pistole HK45C. Všechny druhy střelných zbraní jsou atentátníky využívány ke spáchání teroristického činu na malý počet osob nebo na konkrétní cíl. [18]

Při útoku na konkrétní osobu nebo malý počet osob, se využívá i chladných zbraní, jakými jsou například meče, nože, sekery, dýky apod. Chladné zbraně jsou tiché, ve většině případů lehce maskovatelné. Navíc konkrétně nůž a jeho opatření a držení není v rámci české legislativy nijak regulován. [19, 20]

Jako efektivní forma metody spáchání útoku o velkém rozsahu na osoby, symbolické, významné, historické nebo měkké cíle, je využití výbušniny. Samotný rozsah škody a s tím i obavy, které tento typ útoku s sebou přináší, umožňuje teroristům s veřejností manipulovat i ve formě planých hrozeb. Tyto falešné útoky na daný objekt vedou k vyklizení objektů a tím pádem volné pole působení útočníků. K oblíbeným typům výbušnin ze široké škály, patří například Semtex 1A, Trinitrotoluen a C-4. A jednotlivé typy se liší i v rychlosti detonace či vlastností samotné výbušniny. [21]

- Moderní

Spolu s vývojem technologií a pokroku ve vědě se rozšiřuje i spektrum hrozeb, kterým Česká republika může čelit. Za odvětvími, která se zabývají genovou manipulací, biologickými modifikacemi a chemickými pokusy se nacházejí fyzické osoby, vědci, jejichž informace by mohly být lehce zneužitelné pro uskutečnění teroristického útoku. [20]

Na druhou stranu by použití zbraní hromadného ničení přineslo mnohé negativní faktory, jako například následná dlouhodobá nehostinnost prostředí, kde by byl útok realizován. Možná právě proto se zbraně hromadného ničení využívají hlavně pro udržení veřejnosti v konstantním strachu a jako nátlakový prostředek na vládu, instituce a organizace. K dalším moderním metodám útoku patří bezpilotní letouny. V armádě se tento typ prostředku využívá již delší dobu a je otázkou, do jaké míry tuto metodu využívají teroristické skupiny například pro fázi plánování útoku. Další, dosud nevelmi prozkoumanou hrozbou, jsou

zbraně zvukové, které fungují na bázi ultrazvukových a infrazvukových vln, které mohou zásadně poškodit kardiovaskulární systém zasažených osob. [20, 22]

Vývoj četnosti jednotlivých teroristických útoků zaznamenává níže přiložený seznam útoků. Seznam je založen na datech, vycházejících ze statistiky Global Terrorism Database a vyhodnocuje údaje za 16 let vztahující se k teroristickým útokům (vykonaných i nedokončených) na území evropského kontinentů od roku 1998. Jednotlivé položky jsou seřazené sestupně, dle četnosti. [20, 25, 29]

- Útok výbušninou,
- Sebevražedný útok,
- Výbušnina v poštovní zásilce,
- Výbušnina v zaparkovaném vozidle,
- Nájezd vozidla s výbušninou se sebevražedným útočníkem,
- Žhářský útok,
- Útok střelnou zbraní,
- Braní rukojmí a barikádová situace,
- Napadení chladnou zbraní,
- Napadení měkkého cíle davem
- Útok nájezdem vozidla. [29]

#### 1.4 Fáze teroristického útoku

Každý teroristický útok organizované skupiny nebo útočníka prochází vývojem, který zahrnuje jako jeden z prvních kroků fázi zhodnocení cíle, na který má být spáchán útok ze stránky lukrativnosti a dosažitelnosti.

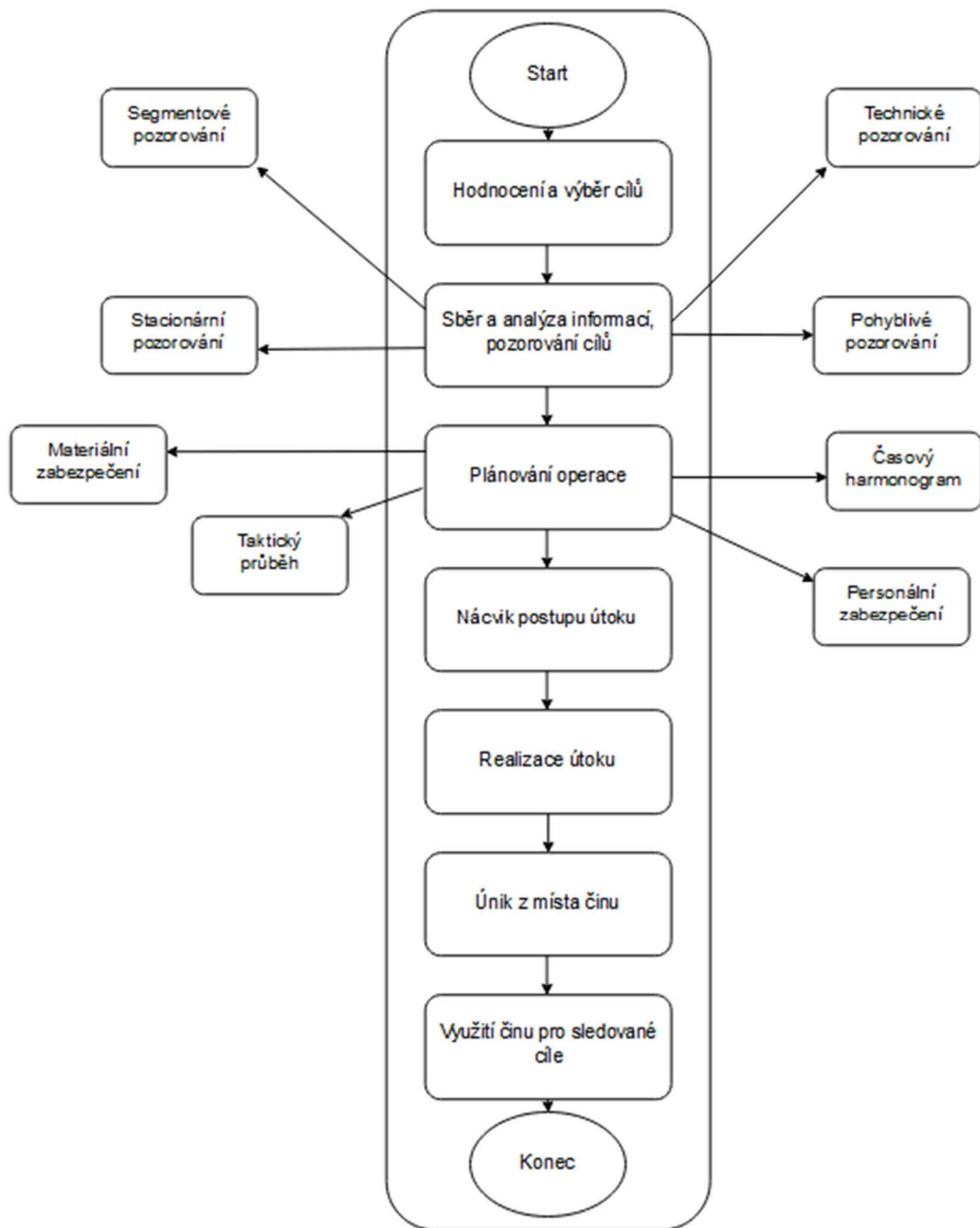
Pro zvolené cíle se dále provede rozbor a shromáždění potřebných informací. Útočník má většinou omezené možnosti pro dosažení informací, tudíž je podstatnou složkou fáze sběru informací pozorování. Typy pozorování lze z hlediska použitých metod a prostředků rozdělit do jednotlivých typů:

- a) Stacionární pozorování – provádí pozorovatel dlouhodobě ze stejné pozice pro zjištění aktivit specifikovaných míst a objektů.
- b) Pohyblivé pozorování – je zajištěno pěšími pozorovateli anebo je využito automobilů. Typickým je pro něj využití k odpozorování konkrétních osob anebo zjištění situace v různých oblastech.

- c) Technické pozorování – je využito k zajištění informací pomocí technických prostředků jako například kamery, odposlouchávací zařízení, optické systémy, apod.
- d) Segmentové pozorování – řadí se k časově nejnáročnějším typům pozorování, kdy se musí zajistit jednotlivé dílčí části pro utvoření celistvého plánu. Využívá se pro náročné získání informací. [23, 24]

Po odpozorování a vyhodnocení potřebných informací nastává krok plánování samotného útoku po stránce časové, materiální, taktické a personální. Pokud se nejedná o sebevražedný čin a útočníci mají vhodné podmínky, přichází do pořadí nácvik útoku. Díky nácviku se ověří funkčnost celého připraveného plánu, časový harmonogram a taktiky.

Realizace plánu vrcholí provedeným útokem, po kterém nachází fáze komplikovanější, než samotný útok – opuštění místa činu. Po jednotlivých fázích se akce teroristického útoku dostává do nejdůležitějšího stádia, ve kterém se zhodnotí účel vykonání celé akce a povětšinou za pomoci médií se interpretuje celková úspěšnost útoku. Teroristé vydávají prohlášení, adresující vládě či významné osobě. Jednotlivé dílčí fáze jsou pro přehlednost zobrazeny na níže přiloženém diagramu na obrázku (Obr. 1). [24]

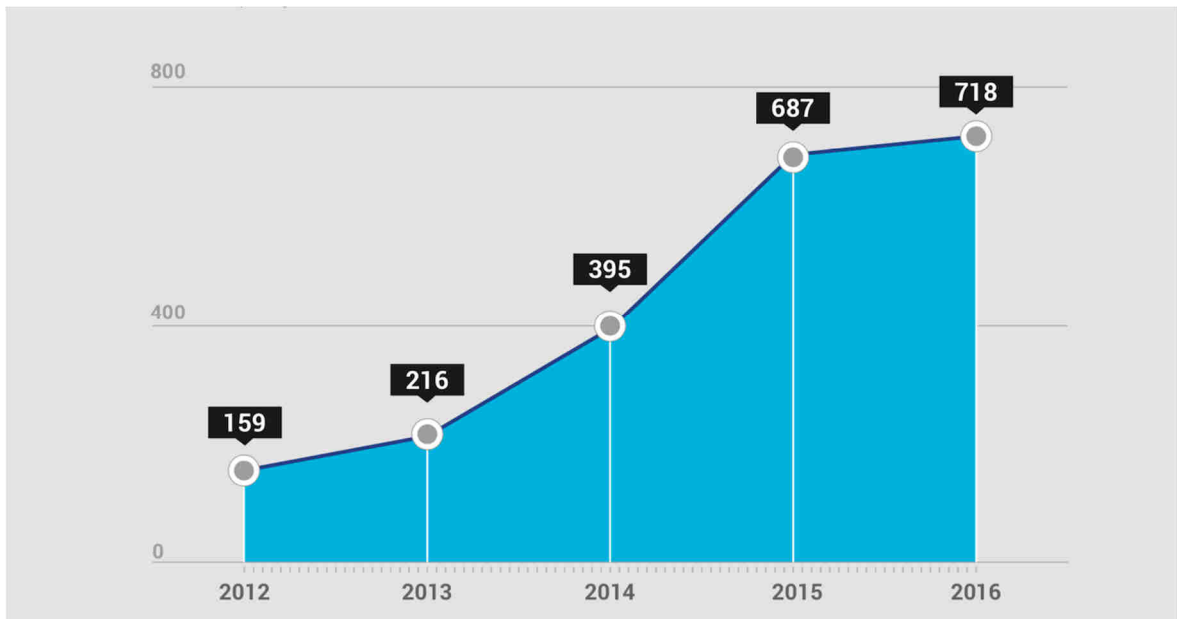


Obr. 1: Fáze útoku [24]

## 1.5 Mapování terorismu

Pro stanovování prognóz, poučení se z historie a popřípadě předpokládání důsledků je velmi nutné zpracování informací. S těmi pracuje veřejná databáze The Global Terrorism Database (GTD), která sbírá a kontroluje veškerá data událostí násilných útoků ve světě. Tato data zpracovává již od roku 1970 na základě získaných informací od celosvětových médií, které uvádí a zahrnuje do databáze až po pečlivém ověření a prokázání pravosti. [25]

Na podobném principu funguje pro Evropskou unii Europol, který se komplexně zabývá trestní činností v EU od roku 2007. Europol pravidelně podává zprávy o aktuální situaci a vývoji terorismu, zabývá se zkoumáním teroristických skupin a organizací a v neposlední řadě se snaží hodnotit a předvídat nové zločinecké hrozby EU. Příkladem je níže přiložený graf přiloženého obrázku (Obr. 2), který zaznamenává nárůst náboženského terorismu mezi lety 2012 a 2016. [25, 26]



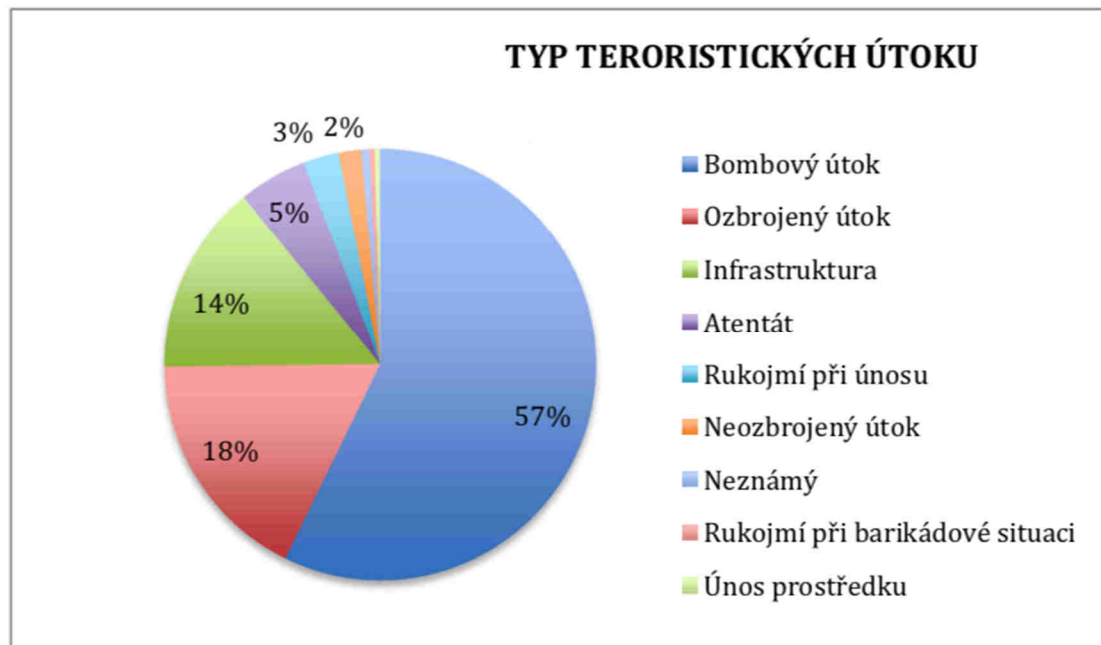
Obr. 2: Počet zatčených podezřelých za náboženský terorismus od roku 2012 do 2016 v Evropské Unii [27]

Z výše umístěného obrázku, obsahující graf, můžeme vidět vzrůstající tendenci náboženských útoků v Evropské unii. Konkrétně bylo v roce 2016 zadrženo 718 osob na podezření z náboženského terorismu a z toho celých 429 bylo zadrženo pouze na území Francie. Jako nový trend se také uvádí počet zadržených žen, kdy stále častěji právě ženy přebírají operační role v džihádistických teroristických činnostech. Konkrétní čísla ukazují, že každý čtvrtý útok je pod záštitou právě ženského pohlaví, což je 18% nárůst oproti roku 2015. [27]

Za rok 2017 bylo provedeno celkově 207 teroristických útoků, které zasáhly 9 členských zemí Evropské unie, což je o více než 60 útoků více, než tomu bylo v roce 2016. Přes polovinu z těchto útoků byla ohlášena Velkou Británií, dalším nejvíce sužovaným státem byla Francie a za ní Španělsko.

Celkově bylo v Evropské unii usmrceno v předminulém roce 68 obětí a zraněno 844. Stejně, jako tomu bylo v předešlých letech, byly škody způsobeny nejvíce důsledkem džihádistických teroristických útoků. [28]

Vývoj v zastoupení jednotlivých druhů teroristických útoků se odráží v analýze zpracovaných dat od roku 1998 do roku 2014 v rámci evropského kontinentu. Celkově vyhodnocení vychází z 5297 údajů a jak je zřejmé z níže přiloženého grafu obrázku (Obr. 3), procentuální zastoupení bombových útoků výrazně převažuje. [29, 30]



Obr. 3: Procentuální zastoupení jednotlivých typů teroristických útoků [29]

## 1.6 Významné teroristické útoky

Následující kapitola obsahuje tabulku (Tab. 2) s výčtem konkrétních teroristických útoků, které se řadí k největším v celé historii. Útoky jsou seřazeny sestupně, podle počtu obětí. Jako útok s největším počtem obětí prozatím zůstává již zmiňovaný útok z 11. září 2001, který byl nejen významným co do počtu mrtvých a zraněných osob, ale také svým důmyslným propracováním a použitím veřejných prvků jako substituci vlastních zbraní. Útok 11. září proto zůstává dnem, kdy téma terorismu začalo být vnímáno širokou veřejností.

Tab. 2: Seznam největších teroristických útoků do roku 2018 [31]

Pořadí	Název útoku	Země	Rok	Oběti	Typ útoku
1	9/11 Attacks	USA	2001	2996	Chladné zbraně a únos letadel
2	Camp Speicher Massacre	Irák	2014	1566	Masová vražda
3	Christmas Massacre	Demokratická republika Kongo	2008	860	Střelba a chladné zbraně
4	Yazidi Communities Bombings	Irák	2007	795	Automobilová nálož
5	Sri Lankan Police Officers Massacre	Srí Lanka	1990	774	Masová vražda
6	Mogadishu Bombings	Somálsko	2016	655	Automobilová nálož
7	Ankara Suicide Bombings	Turecko	2015	508	Sebevražedný útok
8	Cinema Rex Fire	Irán	1978	420	Žhářství
9	Massacre of Trujillo	Kolumbie	1990	400	Masová vražda
10	Karrada Bombing	Irák	2016	342	Automobilová nálož
11	Gamboru Ngala Attack	Nigérie	2016	336	Žhářství a střelba
12	Air India Flight 182 Bombing	Kanada	1985	329	Bombový útok
13	Sinai Mosque Attack	Egypt	2016	311	Bombový útok a masová střelba
14	Beirut Barracks Bombing	Lebanon	1983	307	Automobilová nálož a sebevražedný útok
15	Russian Apartment Bombings	Rusko	1999	293	Bombový útok
16	Pan Am Flight 103	Velká Británie	1988	270	Bombový útok
17	Bombay Bombings	Indie	1993	257	Automobilová nálož
18	As-Suwayda Attacks	Sýrie	2018	255	Sebevražedný útok a střelba
19	Angola Train Attack	Angola	2001	252	Bombový útok
20	Rais Massacre	Algérie	1997	238	Masová vražda
21	Kobani Massacre	Sýrie	2015	233	Sebevražedný útok
22	Metrojet Flight 9268	Egypt	2015	224	Bombový útok

23	United States Embassy Bombings	Tanzánie	1998	224	Automobilová nálož
24	Sadr City Bombings	Irák	2006	215	Automobilová nálož
25	Mumbai Train Bombings	Indie	2006	209	Bombový útok
26	Bali Bombings	Indonésie	2002	202	Sebevražedný útok a automobilová nálož
27	Bentalha Massacre	Indie	2008	174	Bombový útok a střelba

## 1.7 Terorismus v České republice

Vzhledem k poloze demokratické České republiky v prostředí okolních států se stejnou formou vlády by se dalo tvrdit, že se jedná o polohu s dobrými podmínkami pro dlouhodobě udržitelnou národní bezpečnost. Navíc se jedná o zemi, která se příliš nerozčleňuje ani v otázce vyznávání náboženství – přes 75 % Čechů se nehlásí k žádnému vyznání a 23 % jsou křesťané. [32]

I přes tato světlá fakta nemůžeme spoléhat na trvale udržitelnou situaci už jen z důvodu několika společenství, která Česká republika udržuje a se kterými je součástí – jako například Severoatlantická aliance a Evropská unie. Právě tato společenství by mohla být například jedním z prvků, poutající pozornost teroristů, jelikož vše, co se stane v Evropě, se promítne do osudu českého národa. Vzhledem k těmto původům myšlenek k zaútočení, lze terorismus rozdělit do dvou skupin:

- Domácí terorismus

Jedná se o terorismus, jehož myšlenka vznikla na území České republiky a s převažujícím působením domácích faktorů. Často se jedná o nesouhlas s politickou situací, představitele vlády či v dnešní době velmi diskutované téma rozdělovací společnost – Evropská migrační krize. Konkrétním příkladem domácího terorismu se zárodkem v migrační krizi je útok z roku 2018, kdy sedmdesátiletý český důchodce Jaromír Balda měl za cíl podněcovat v obyvatelích státu nedůvěru až xenofobii z migrantů, jenž v posledních letech do Evropy přichází. K dosažení svých cílů volil ze začátku distribuci výhružných letáků v arabském jazyce, které se později proměnily v reálný teroristický čin ve formě pokácení stromů na železniční dráhy, což způsobilo havárii dvou vlaků. [7, 33]



- Importovaný terorismus

Importovaný terorismus neboli terorismus, jehož myšlenka nemá původ na území České republiky a byla do země přivedena ze zahraničí. Jak již bylo řečeno výše, prvním rizikem vedoucím k importovanému teroristickému útoku je členství České republiky v mezinárodních organizacích, jakými jsou například Evropská unie a Severoatlantická aliance a také příslušnost České republiky k západnímu civilizačnímu okruhu, který je asociován převážně Spojenými státy a evropskými mocnostmi, jakými jsou Francie, Velká Británie či Německo. Právě tyto mocnosti byly v historii již několikrát sužovány teroristickými útoky a pozornost, kterou na sebe strhávají spolu se společenstvím, které s nimi Česká republika uchovává, z ní může vytvořit druhotný cíl pro teroristy, v jejichž zájmu by bylo například zničení demokracie či západních hodnot. [34, 35, 36]

## 1.8 Teroristické organizace

Většina teroristických organizací má pyramidovou strukturu, kdy v horní části můžeme nalézt tvrdé jádro skupiny, které vybírá cíle, zpracovává informace a připravuje plány, poté střední část, kde se nacházejí aktivní členové, kteří provádějí útoky za tímto účelem a operují v malých buňkách lidí a řeší zpravidla praktické fungování organizace jako například obstarávání zbraní, falšování dokladu, obstarávání financí, dopravních prostředků apod. A ve spodní části pyramidy se poté nachází pasivní sympatizanti, kteří vyjadřují přízeň organizaci a slouží také jako prostředí pro nábor nových členů organizace. [7, 24, 37]

Tato podkapitola přibližuje na základě výčtu informací nejznámější teroristické organizace v moderní historii.

- Euskadi ta Askatasuna

Španělská teroristická skupina založena roku 1959, známá pod zkratkou ETA, usilující o vznik samostatného baskického státu. Kořeny zakladatelů sahají do oblasti Kavkazu a jsou příslušníky velmi starého národa. Od 16. století organizují destruktivní akce, které měly pomoci splnit cíl. Útoky ETA jsou zaměřeny především proti španělským vládním institucím a obzvlášť proti španělskému bezpečnostnímu aparátu. K finančním prostředkům organizace přichází obzvlášť z nezákonných forem, jakými jsou vydírání a loupeže. Velkou pozornost organizace upoutala bombovými útoky na rekreační centra. K roku 2014 skupina oznámila ukončení ozbrojeného boje. [37, 38]

- Islámské hnutí odporu

Jedná se o odnož islámské organizace Muslimští bratři, také známou jako Hamas, kdy doslovný překlad z arabštiny zní “nadšení”. Vznikla ve dvou uskupeních. První je tajná vojenská složka útočící v Izraeli. Druhá část se soustředí na politické a civilní cíle, rekrutuje a poskytuje sociální služby. Skupina se zapojila do boje proti Arafatově uskupení a začala okupovat tato území.

Cílem Hamasu je vybudovat nezávislý stát na území dnešního Izraele. Hamas má díky obrovskému ideálu tisíce příznivců, jež jsou ochotni a schopni skupinu financovat členskými příspěvky. Skupina má schopnost oslovit mladé lidi, a získat podporu i mimo území Izraele. V lednu 2006 například Hamas vyhrál volby do Palestinské národní správy. Finanční prostředky organizace dostává od emigrantů, z Íránu a například od soukromých osob v Saúdské Arábii. Výrazným znakem skupiny je rozsáhlá propaganda a hrubé násilí, které používá k dosažení svých cílů. [37, 39]

- Irská republikánská armáda

Irská republikánská armáda, s označením IRA, je polovojenské hnutí, které usiluje o to, aby se Irsko stalo samostatnou republikou. Irští dobrovolníci jsou známí pod názvem „Sin Féin“. Jedná se však o ozbrojenou složku, která pro vznik samostatného státu usiluje taktéž násilím. Ve 30. letech 20. století byla tato skupina postavena mimo zákon a dále působí ilegálně. Britská armáda je dle této skupiny překážkou ve vzniku samostatného Irska. Proto často útočí na vládní představitele, důstojníky armády, a to i formou nástražných výbušných systémů. Jako financování využívají mimo jiné únosy dětí bohatých rodin.

IRA je rozdělena do čtyř skupin. Některé její odnože totiž nesouhlasí s násilím, které skupina provádí – typické jsou pro ně vraždy, bombové útoky a vydírání), a proto došlo k rozdělení. V dubnu roku 1998 se IRA dobrovolně vzdala svého arzenálu a stala se částečně legální politickou silou a tím ukončila svou ozbrojenou činnost. [37, 40]

- Čínské triády

V dávné minulosti byly triády jednou ze tří hlavních tajných sdružení. Vytvořila odvětví v Macau, Hong Kongu, a Taiwanu. V místech, kde se vyskytuje početná čínská populace, se vyskytují další odnože, a to například ve Francii, Španělsku, Severní Africe, Austrálii, Brazílii, Velké Británii a v dalších státech. [3, 41]

„Počátky jedné z nejstarších teroristických organizací sahají do doby 220 až 206 před n.l. Organizace se vyznačovala nejvyšším stupněm utajení, což bylo typické pro celou řadu 19 organizací a spolků v Číně. Slovo triáda znamenalo, že došlo ke spolupráci třech tajných organizací. Tři organizace měly ve znaku člověka, nebe, zemi. Členem se mohl stát pouze člověk, který splnil krevní přísahu mimo jiné přečtením svazků třiceti knih“. [6]

- Al-Káida

V doslovném překladu „základna“. Jedná se o militantní sunnitskou islámskou organizaci, která byla založena v roce 1988. Zakladatelem byl Usáma Bin Ládín, Abdullah Azzam a několik arabských dobrovolníků během sovětské invaze v Afghánistánu. Al Káida se přihlásila k útoku na americké obchodní centrum World trade center.

K financování svých aktivit využívají prodej drog, krádeže, únosy a často také vydírání. Některé zdroje naznačují, že islámské teroristické skupiny jsou financovány z Turecka, Saúdské Arábie, nebo Kataru. Jako úhlavní nepřítel jsou označeny Spojené státy americké a všichni jeho spojenci. Organizace má velmi dobrou finanční základnu a vysokou míru přístupu k utajovaným informacím. Po zabití Usámy Bin Ládina skupinu vede Egyptan Ayman al-Zawahiri. [42, 43]

- Islámský stát v Iráku a Sýrii

Islámský stát v Iráku a Sýrii se zkratkou ISIS patří v dnešní době k nejvíce skloňovaným pojmem v souvislosti s útoky na území Sýrie. Odtud původní název Islámský stát v Sýrii a Levantě. V zahraničí nazýván Daesh. V dnešním období patrně nejaktivnější teroristická organizace, s kterou se vedou rozsáhlé boje téměř konvenčního charakteru. Donedávna okupoval velké území a významná města v Sýrii.

Věrnost této organizaci složily také významné teroristické organizace jako například Boko Haram. Je nechvalně známá prosazováním přísného islámského vyznání a práva Šaría. Páchají kruté násilnosti na civilním obyvatelstvu, Šíitech a vyznavačích odlišných náboženství, případně ateistech. [44]

- Boko Haram

Organizace, jejíž oficiální název je „People of the Sunnah“, konající činy pod myšlenkou, že západní vzdělání je hřích. Boko Haram působí převážně v Africe. Útočí především na

křesťany. V roce 2015 obsadili vojenskou základnu u města Baga a způsobili rozsáhlý masakr civilistů. Jejich útoky se vyznačují vysokou brutalitou, přepadáním především dívčích škol a některé jejich útoky hraničí s genocidou. [45]

- Talibán

Talibán, v překladu z perštiny „studenti“, což vystihuje složení organizace, kdy většina stoupců vzešla právě z řad studentů pod vedením učitelů v islámských náboženských školách. Toto radikální nábožensko-politické hnutí v letech 1996–2001 reálně vládlo na většině území v Afghánistánu. Po intenzivním zásahu americké armády se členové Talibánu stáhli do odlehlejších oblastí země, avšak po postupném stáhnutí amerických vojenských jednotek se opět dostává území Afghánistánu pod moc Talibánu. [35, 46]

## 1.9 Boj proti terorismu

Terorismus a otázky a problémy ohledně něj se řeší v několika úrovněovém spektru. V základu je zajištěn boj v jednotlivém státu, konkrétně tedy v České republice pomocí zákonů. Další vrstvou, která pomáhá s bojem proti terorismu, má mezinárodní povahu a spadají do ní země Evropské unie. Poslední úroveň spojuje i mimoevropské státy a pojímá o terorismu jako o globálním problému. [34]

- Vnitrostátní

V České republice se problematika terorismu řeší v několika úsecích. Obecným dokumentem v České republice zabývajícím se terorismem je Bezpečnostní strategie České republiky, kde jsou stanoveny základní prvky bezpečnosti. Tento dokument bývá obměňován dle potřeb a proměn situace ve státě.

Specifičtějšími principy problematiky se poté zabývá Strategie České republiky pro boj proti terorismu. Nejaktuálnější update Bezpečnostní strategie České republiky proběhl v roce 2015, kde se uvádí terorismus jako hrozba. Dále se vyzdvihuje nutnost zapojení České republiky do Společné zahraniční a bezpečnostní politiky Evropské unie a účast v misích pro boj proti terorismu – Společné bezpečnostní a obranné politiky. [7, 34, 36]

- Evropský

Evropský kontinent je rozdělen do několika rozdílných států, které se liší i zákony. Co se týče problematiky terorismu, je zapotřebí maximální spolupráce, a proto vznikla řada orga-

nizací, která se zabývá opatřeními potřebných pro boj proti terorismu. Mezi jednotlivé organizace patří Rada Evropy, Evropská unie, Severoatlantická aliance a Organizace pro bezpečnost a spolupráci v Evropě. [34]

- Globální

Globální úroveň se zabývá opatřeními proti terorismu, která překračují evropskou úroveň. Konkrétně se jedná o tři formy uzavřené spolupráce. První spoluprací České republiky je Organizace spojených národů, dále spolupráce na úrovni G8 a Globální fórum proti terorismu. [7, 34]

### **Dílčí závěr**

I když definice terorismu není jednotná, jeho následky již po mnoha staletí pronikají do mnoha společenských vrstev a nepřímo se tak podílí na ovlivnění dění a vývoje celého lidstva.

V dnešní době jsme schopni rozčlenit vývoj terorismu do jednotlivých ér (primitivní, pokročilý, moderní a postmoderní) a popsat charakteristické prvky jednotlivých období zvlášť. Dle motivace útočníků pro vykonání teroristického útoku rozdělujeme terorismus na Ultralevicový, Ultrapravicový, Etnický, Náboženský, Ekologický a Jednopoložkový neboli tzv. Single-issue terorismus.

Díky údajům, pravidelně verifikovaných a uveřejněných marylandskou univerzitou v databázi The Global Terrorism Database, jsme schopni mapovat teroristické útoky a vytvářet na jejich údajích bezpečnostní prognózy. Údaje a poznatky z nejhorších teroristických útoků (11. září 2001, Camp Speicher Massacre, Christmas Massacre, aj.) nám pomáhají v represivních opatřeních, detekci fází teroristických útoků a odhalení teroristických organizací.

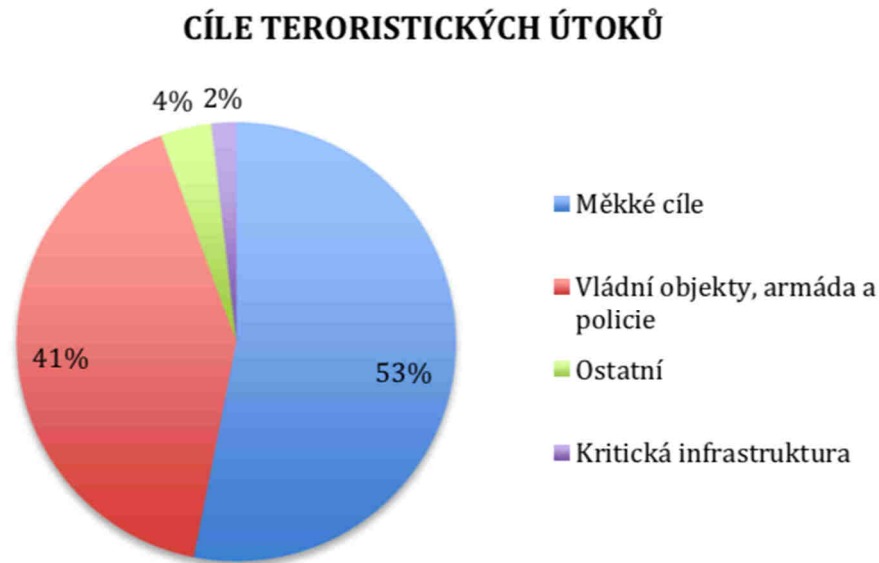
## 2 MĚKKÉ CÍLE

Terminologický slovník Ministerstva vnitra České republiky, definuje měkké cíle jako „Veřejně frekventovaná místa, snadno napadnutelné objekty nebo místa nevojenského charakteru, která nejsou permanentně střežena ozbrojenými složkami nebo jiným způsobem, případně nejsou střežena vůbec. Takováto místa a objekty se vyznačují zejména stálou nebo dočasně vysokou koncentrací osob, symbolickým, kulturním či náboženským významem nebo tvoří významnou součást infrastruktury státu, jejíž narušení má negativní dopad na fungování systému a tím i na společnost.“, avšak nejedná se o oficiální, celosvětově uznávanou definici. Tematika měkkých cílů anebo zaužívaný pojem z anglického sousloví „Soft Targets“, začala být velmi diskutovanou v souvislosti s vzrůstajícím počtem teroristických útoků. [47]

Samotná metoda ochrany měkkých cílů je velmi výjimečná, jelikož při zajištění ochrany zohledňuje pouze pravděpodobnost výskytu události a dává do pozadí celkový dopad či význam pro zemi, společnost nebo vládu. Díky řešení dopadu potencionálního útoku pouze z omezeného/výsečovitého řešení dopadu potencionálního útoku, se dostávají do popředí pomyslného žebříčku pro posílení bezpečnosti i objekty, které spadají do oblastí ne příliš významné pro stát, jakými jsou například obchodní centra, fotbalové stadiony či jiné komerční objekty. [29]

Opakem Soft Targets jsou tzv. Hard Targets, mezi jejichž zástupce patří například armádní budovy, budovy vlády anebo jiné objekty s obecně zpřísněným režimem bezpečnosti. [48]

Zaměření teroristů na měkké cíle potvrzuje také analýza teroristických útoků, která vychází z dat sesbíraných za 16 let v rámci evropského kontinentu od roku 1998. Celkově tedy vyhodnocení vychází z 5297 údajů a jak je zřejmé z níže přiloženého grafického znázornění na obrázku (Obr. 4), měkké cíle jsou bodem zájmu útočníků, a proto by měl být kladen důraz na jejich ochranu. [25, 29, 49]



Obr. 4: Procentuální vyjádření cílů teroristických útoků [29]

## 2.1 Terminologie z oblasti bezpečnostní politiky měkkých cílů

Následující podkapitola odkrývá seznam terminologických pojmů z oblasti bezpečnostní politiky měkkých cílů. Ke každému jednotlivému termínu je připojena stručná charakteristika jeho významu.

- **Aktivum** – vše, co má pro daný referenční objekt hodnotu. Může být snížena působením hrozby. V rámci ochrany měkkých cílů jsou do aktiv zahrnuty osoby, potažmo lidské zdraví a životy.
- **Analýza rizik** – systematická metoda identifikace aktiv, hrozeb vůči těmto aktivům a zranitelnosti systému vzhledem k příslušným hrozbám
- **Bezpečnost** – stav, kdy je dosažena požadovaná úroveň ochrany osob, hmotného a nehmotného majetku a informací, nebo proces směřující k tomuto stavu.
- **Bezpečnostní událost** – zjištěná událost, která může způsobit ohrožení bezpečnosti.
- **Bezpečnostní incident** – zjištěná událost, která způsobila ohrožení bezpečnosti.
- **Bezpečnostní manažer** – odborný zaměstnanec, jehož hlavním úkolem je organizovat, řídit a zajišťovat odborné úkoly bezpečnosti v referenčním objektu.
- **Bezpečnostní nedostatek** – zjištěná slabina (zvýšená zranitelnost) bezpečnostního systému, která může vést k bezpečnostnímu incidentu.
- **Bezpečnostní opatření** – postup nebo mechanismus, který snižuje riziko.

- **Bezpečnostní politika** – množina pravidel stanovených bezpečnostní autoritou přijatá k zajištění požadované bezpečnosti.
- **Bezpečnostní riziko** – Možnost, že s určitou pravděpodobností vznikne událost, kterou považujeme z bezpečnostního hlediska za nežádoucí s negativními dopady na osoby, hmotný a nehmotný majetek.
- **Dopad** – výsledek nechtěného incidentu
- **Fyzická ochrana** – opatření použitá pro zajištění bezpečnosti zdrojů proti úmyslným a náhodným hrozbám. Zajištění ochrany osob, hmotného majetku a fyzických aktiv, především objektů, technické infrastruktury, movitých věcí, finančních prostředků v hotovosti, a také bezpečnostních zařízení.
- **Hrozba** – možná příčina nežádoucího incidentu, jejímž následkem může být poškození systému nebo samotného referenčního objektu.
- **Informace** – jakékoliv sdělení, zpráva, poznatek, text, tedy jevy, které mají výhradně znakovou podobu a jejichž cílem je komunikace a výměna mezi zaměstnanci, smluvními stranami a uživateli třetích stran; také je to podmnožina sdělení, která má význam pro příjemce; je zaznamenána na jakémkoli nosiči – zvukovém, obrazovém nebo audiovizuálním a ovlivňuje chování zaměstnance, smluvní strany a uživatele třetí strany; jsou dostupné, když je jich potřeba. Je důležitým aktivem referenčního objektu, které je třeba chránit, tj. zajistit jejich dostupnost, integritu a důvěrnost. Informace má svůj životní cyklus, vytvoření (tištěná, psaná na papíře nebo elektronicky, verbálně sdílená), uložení (elektronicky, na magnetické nebo jiné medium nebo v tištěné podobě), zpracování, přenášení (poštou nebo elektronicky, na magnetickém nebo jiném médiu), poškození, ztracení, zničení. Informací není počítačový program.
- **Personální bezpečnost** – zajištění ochrany před náhodným nebo úmyslným selháním osob.
- **Riziko** – pravděpodobnost, s jakou určitá hrozba využije určitou zranitelnost aktiva nebo skupiny aktiv a zapříčiní tak poškození nebo ztrátu tohoto aktiva. Je to možnost, která může či nemusí nastat, a která má svým dopadem vliv na referenční objekt, skupinu či jednotlivce, že daná hrozba využije zranitelnosti aktiv nebo skupiny aktiv a způsobí tak ztrátu nebo zničení aktiv, je to kombinace pravděpodobnosti výskytu událostí a jejich následků. Riziko lze chápat pozitivně (generuje příležitosti) i negativně (je příčinou ztrát). Faktor dopadu rizika je založen na ocenění aktiva.
- **Řízení rizik** – proces rozpoznávání, kontroly, minimalizace a odstraňování rizik



- **Měkký cíl (Soft Target)** – veřejně frekventované místo, snadno napadnutelný objekt nebo místo nevojenského charakteru, které není stráženo ozbrojenými složkami nebo jiným způsobem. Charakterizuje se zejména dlouhodobě nebo dočasně vysokou koncentrací osob.
- **Správci objektů** – odborní zaměstnanci pro personální, administrativní a fyzickou bezpečnost a pro ochranu životního prostředí a prevenci závažných havárií, bezpečnost a ochranu zdraví při práci a požární ochranu v referenčním objektu, jejichž hlavním úkolem je organizovat, řídit a zajišťovat odborné úkoly bezpečnosti v rámci jejich působnosti. Správci objektů jsou určeni bezpečnostním manažerem z vedoucích zaměstnanců Fakulty aplikované informatiky.
- **Zodpovědnost** – vlastnost zajišťující, že činnosti určitého subjektu bude možné vysledovat.
- **Zranitelnost** – Zranitelnost je označení slabiny či nedostatku aktiva, které umožňuje uplatnění hrozby. Zranitelnost aktiva je úzce spjata se schopnostmi a dovednostmi pachatele napadnout dané aktivum. Zranitelnost závisí na typu a vybavení útočnicka. Obecně lze předpokládat útočnicka s prostředky a znalostmi k úspěšnému provedení útoku na zvolený cíl. Konkrétní zranitelnost závisí na povaze a konstrukci potencionálního cíle s možností maximalizovat efekt úsilí útočnicka pomocí místního vybavení. [50, 51, 52, 53, 54]

## 2.2 Útoky na měkké cíle v ČR

Útoky na měkké cíle na území České republiky naštěstí dosud nemají příliš bohatou historii. Také oběti, podléhající pod tento druh násilného činu, jsou ve srovnání s útoky v Evropě pouze malou výsečí. Zatímco k prozatím nejtragičtějším útokům v České republice patří střelba v restauraci Družba v Uherském Brodě, kde vlivem útoku přišlo o život osm osob. V kontextu evropských útoků na měkké cíle lze zmínit například útok v Nice (Francie), kdy v roce 2016 v důsledku teroristického útoku spáchaného v období národních oslav, bylo nájezdem kamionu usmrceno 87 osob včetně dopadeného útočnicka. [55, 56]

Dalším významným datem je 19. prosince 2016, kdy v době předvánočních oslav na největším náměstí v Berlíně (Německo), útočník vjel kamionem naloženým ocelovými deskami do prostoru vánočních trhů a zranil 60 osob, z nichž 12 svým zraněním podlehl. Tabulka (Tab. 3) zaznamenává útoky na měkké cíle na území České republiky s konkretizovanými údaji obětí, místa činu, data útoku a jmény útočníků. [57]

Tab. 3: Útoky na měkké cíle na území ČR do roku 2016 [55, 58, 59]

Pořadí	Místo	Rok	Útočník	Oběti	Útok
1	Metro C, Praha	2005	Viktor Kalivoda	0 (včasný zásah policie)	Střelba
2	Tiskárna Gaspro, Zlín	2009	Bývalý zaměstnanec	1 mrtvý, 1 zraněný	Střelba
3	Aircraft Industries, Kunovice	2011	Karel Musela	3 mrtví, 1 zraněný	Střelba
4	Obchodní akademie, Žďár nad Sázavou	2014	Barbora Orlová	1 mrtvý, 3 zranění	Chladná zbraň
5	Restaurace, Uherský Brod	2015	Zdeněk Kovář	8 mrtvých, 1 zraněný	Střelba

### 2.3 Dosavadní aktivity pro ochranu měkkých cílů v ČR

Ochrana měkkých cílů na území České republiky je obecně řešena dokumentem Strategie ČR pro boj proti terorismu. Jako reakce na přibývajících teroristické útoky s převážnou většinou na měkké cíle, byla zpracována celistvější forma řešení problematiky a bylo sepsáno Memorandum o spolupráci v rámci sdílení informací bezpečnostních složek o určitých typech útoku, které bylo odsouhlaseno zástupci krajů a obcí na začátku roku 2016. [47]

Zaznamenané útoky na měkké cíle za poslední dobu nám odkrývají fakt, že útočníci na měkké cíle nemusí v zásadě patřit k teroristickým organizacím. Zranitelnost měkkého cíle je natolik velká, že zaujala pozornost i útočníky násilné trestné činnosti. (útok v Uherském Brodě).

Během poslední doby proběhlo několik různých seminářů a školení jednotek policistů krajského ředitelství zaměřených na ochranu měkkých cílů. V souvislosti s podporou ochrany měkkých cílů byla zpracována technická norma ČSN 73 440022 Prevence kriminality – řízení bezpečnosti při plánování, realizaci a užívání škol a školských zařízení, která se zaměřuje na ochranu škol a školských zařízení z pohledu měkkých cílů. [47]

Dále vznikla koncepce ochrany měkkých cílů pro roky 2017-2020, jejímž cílem je vytvořit fungující národní systém ochrany měkkých cílů, díky kterým bude možno plošně zlepšit odolnost a prevenci měkkých cílů. Roku 2017 poprvé zasedl stálý poradní sbor Ministerstva vnitra České republiky pro ochranu měkkých cílů. Nedílnou součástí jsou také neinvestiční dotace, zřízeny jednotlivými ministerstvy (doprava, kultura, vnitra, zdravotnictví), které budou realizovány v letech 2019–2021. [7, 29, 47]

Dosud zveřejněné dokumenty v souvislosti s problematikou ochrany měkkých cílů:

- Metodika ochrany měkkých cílů,
- Bezpečnostní standard k ochraně měkkých cílů,
- Koncepce ochrany měkkých cílů pro rok 2017-2020,
- Brožura – 10 principů z odolnosti měkkého cíle,
- Bezpečnostní standardy pro pořadatele sportovních, kulturních a společenských akcí,
- Bezpečnostní doporučení,
- Informační kampaň – ochrana měkkých cílů,
- Vyhodnocení ohroženosti měkkého cíle,
- Bezpečnostní plán měkkého cíle. [7, 29, 47, 49]

### **Dílčí závěr**

V závislosti na přibývajících teroristických útocích začala být diskutována tematika ochrany měkkých cílů. Na základě údajů z množství spáchaných útoků jsme schopni hodnotit objekty a situace, které mají faktor (velké kumulace lidí na málo zabezpečeném prostranství s malou ochranou) a charakter lehkého cíle pro útočníky.

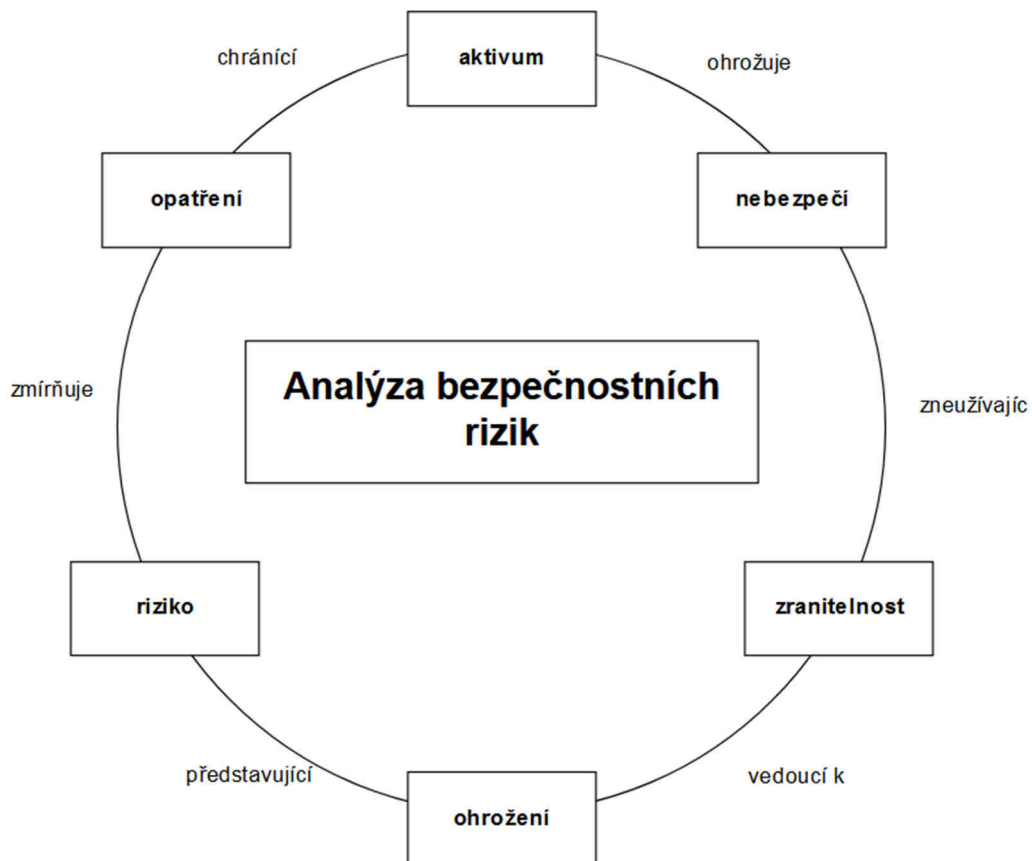
V České republice se počet útoků na měkké cíle úspěšně drží pod kontrolou díky prevenci a včasným zásahům policie. I přesto Česká republika plošně bojuje pro zlepšení ochrany měkkých cílů pomocí metodik, bezpečnostních standardů, doporučení a norem.

### 3 ANALÝZA RIZIK

Analýzou rizik můžeme chápat hledání podstaty vzniku rizika v kontextu nebezpečí a jeho dopadu na život, zdraví a majetek (společnosti či jednotlivce). Základem analýzy rizik je systematické získávání a využívání dostupných informací s cílem určení četnosti daného jevu, jeho intenzity a možných následků. Při aplikování metod jde zejména o porovnání a analyzování různých faktorů vnitřního a vnějšího prostředí, jevů a procesů, které jsou za určitých podmínek schopné narušit či poškodit funkce daného systému, či znemožnit dosažení stanoveného cíle.

Cílem analýzy rizik je také vědecky prognózovat budoucí projevy a důsledky vědeckých metod, které se opírají především o získané objektivní a relevantní fakta o daném ohroženém systému. Prognózovat jeho chování jako celku v nejrůznějších krizových situacích a definovat způsoby jeho spontánní či řízené reakce. Na rozdíl od jiných analýz, analýza rizik přistupuje a probíhá k danému jevu ve smyslu prevence, výsledek je tedy aplikován v různých podobách krizových plánů.

K analýze rizik se také pojí hodnocení rizik, které se provádí na základě verifikovaných, pravdivých a konkrétních informací a datech v konkrétních případech ohrožení – teroristický útok, živelná pohroma, havárie apod. pro specifikované místo a definovaný čas. Hodnocení rizik přispívá k zajištění správného rozhodování a optimálních výstupů analýzy rizik. Jednotlivé faktory vstupující do analýzy rizik a jejich souvislosti jsou graficky znázorněny obrázkem (Obr. 5). [50, 60]



Obr. 5: Grafické znázornění analýzy rizik [60]

### 3.1 Všeobecné přístupy k obsahu analýzy rizik

Pro řízení rizik je důležitá soustavná analýza a hodnocení jeho kvalitativních a kvantitativních parametrů. Riziko obsahu analýzy je vždy vázané k člověku a jeho skutečnou hodnotu lze poznat až po konkrétním vykonání a následném projevení. Mezi základní přístupy k realizaci analýzy rizik jsou nejčastěji zařazovány:

- Identifikace aktiv,
- Stanovení hodnoty a seskupení aktiv,
- Identifikace hrozeb,
- Analýza hrozeb a zranitelnosti,
- Stanovení pravděpodobnosti jevu,
- Měření rizika,
- Stanovení hranice analýzy rizik – pomyslná hranice aktiv zahrnutých a nezahrnutých do analýzy. [60, 61]

- Identifikace aktiv

Identifikace aktiv spočívá v tom, že je vytvořený inventář veškerých aktiv, které leží uvnitř pomyslné hranice analýzy rizik. Přitom jsou jednotlivá aktiva uvedena podle zvolené logiky. Konkrétně jde o posouzení toho, co může být v systému ohrožené, jak to může být ohrožené a proč právě dané aktivum může být ohrožené. [60, 61]

- Identifikace rizik

Identifikace rizik se může realizovat i prostřednictvím podrobnějšího popisu. Na identifikaci rizik se využívá celá řada postupů a technik, včetně kontrolních seznamů, posudků vycházejících ze skutečností a záznamů, vývojových diagramů, výsledků tzv. brainstormingu, systémové analýzy, analýzy scénářů a systémových inženýrských technik.

Použitá metoda bude záviset od charakteru uvažovaných činností a od druhu rizika. Pro získání komplexnějšího výsledku je vhodné použít několik navzájem se doplňujících metod. Jedná se o nacházení odpovědí na otázky co, kolik a kdo nás ohrožuje vzhledem k našim prostředkům a schopnostem odolat. Správné odpovědi jsou závislé na míře získaných informací, jelikož riziko, které není identifikované, nemůže být ani řízené. Proto se také obsah identifikace dále člení na otázky:

- |                                   |   |
|-----------------------------------|---|
| - Co a kolik se toho může stát?   | - Jaké povahy je toto riziko?               |
| - Kde a kdy se to může stát?      | - Jakou intenzitou nás zasáhne?             |
| - Jakým způsobem se to může stát? | - Má riziko potenciál růstu?                |
| - Proč se to může stát?           | - V jakém prostředí a čase riziko existuje? |

- Posouzení zranitelnosti

Při vymezování zranitelnosti je nevyhnutelné zvažovat různé aspekty zranitelnosti ohroženého systému, hustoty obyvatelstva a charakter osídlení či rozmístění obyvatel ve vztahu k ohrožení. Dále je důležitým aspektem specifická zranitelnost různých skupin (ekonomické, náboženské, etnické) a zvážení dislokace zařízení či referenčního objektu také v souvislosti s umístěním složek Integrovaného záchranného systému a životně důležitým objektem (zdroj energie a vody). V neposlední řadě je patřičné se zamyslet nad odhadem primárních a sekundárních důsledků destrukce. [60, 61, 62]

- Vymezení zvládnutelnosti

Dalším krokem analýzy rizika ohroženého systému je vymezení zvládatelnosti tohoto rizika a jeho opatření při řešení tohoto problému se osvědčilo respektování takového postupu, který

by umožnil co nejvšestrannější analyzování všechny obranné a ochranné parametry ohroženého systému.

- Řízení rizik

Jedním z důležitých předpokladů jakékoliv lidské činnosti je „zvládnutí“ rizika, které se pojí s vykonáváním dané činnosti. V souvislosti s tím je nevyhnutelné předvídání budoucího vývoje, ve kterém by se mohlo riziko projevit a ve kterém by mohlo dojít k uskutečnění hrozby tím, že dojde k aktualizaci nebezpečí v systému. Takovouto kontrolu rizik můžeme chápat jako cílevědomé, systematické snižování rizik na akceptovatelnou míru anebo úplné akceptování rizika bez pokusu o jeho snížení. [53, 63, 64]

- Ošetření rizik

Ošetření rizik zahrnuje výběr jedné nebo více možností pro změnu tzv. modifikování rizik a jejich zavedení. Možnosti pro ošetřování rizik by se neměly navzájem vylučovat. Možnosti pro ošetření rizik zejména obsahují vyvarování se rizika rozhodnutím nezačínat nebo nepokračovat s činnostmi, které dávají vzniknout riziku, snížení rizika na základě přijetí vhodných protiopatření, změnu následků nebo omezení zranitelností a v neposlední řadě vyhnutí se riziku. [63]

- Určení zdrojů možných ohrožení

Zdroje možného ohrožení souvisí s identifikací rizikových faktorů externího a interního prostředí. Dále identifikací oblastí posouzení zranitelnosti objektu, ohrožených míst v něm a posouzení faktorů analýzy rizik a jejich možných vlivů při realizaci uvažovaných variant řešení hledání bezprostředních příčin možného negativního jevu.

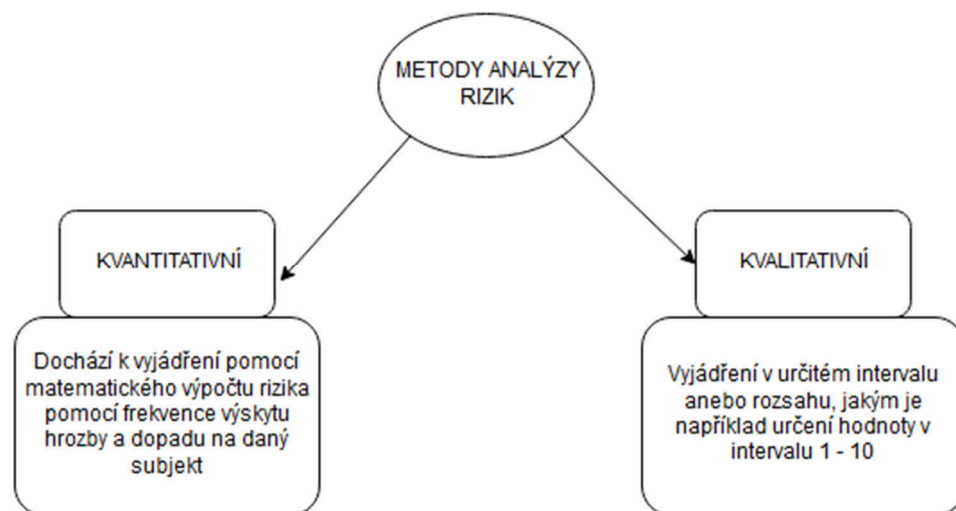
## 3.2 Metody analýzy rizik

K analýze rizik se používá řada různých metod a v dnešní době i softwarových nástrojů. Jednotlivé metodiky jsou založeny na fyzikálních modelech, které se liší svou složitostí a členitostí. V závislosti na složitosti se poté liší správnost a spolehlivost výstupů. Ve většině případů vznikly pro potřeby odhalení rizik pro konkrétní společnosti či instituce.

Jednotlivé metody lze rozdělit z různých úhlů pohledů, jedním z nich je rozdělení na indukční a dedukční. Kdy indukční metody umožňují předvídat poruchu zařízení v ucelené

provozní soustavě, analýza poukáže na možné vlivy, které mohou poruchy zapříčinit a zároveň vyhodnotit následek poruch a následně přijmout vhodná opatření. Zatímco metody dedukční analyzují vzniklé nehody a zkoumají souvislosti, kvůli kterým vznikly.

Metodiky lze také rozdělit na kvalitativní a kvantitativní – jak je zaznamenáno v diagramu obrázku (Obr. 6) níže. Kvalitativní metody se obecně využívají v případech, kdy se jedná o jednoduché situace anebo při nesnadno vyjádřitelných číselných hodnotách. Pomocí této metody lze hodnotit riziko jako například přijatelné/ nepřijatelné, nízké/ vysoké apod. Na druhou stranu metoda kvantitativní využívá číselný charakter hodnot pro evaluaci rizik pro vyjádření pravděpodobnosti, množství, míry apod. Využívá se především při nedostatku relevantních údajů, které se dají hodnotit statisticky. Výsledná kvalita analýzy se odvíjí od přesnosti a úplnosti vstupních číselných hodnot. Následky možných událostí je možné posoudit modelováním výsledků. [50, 60]



Obr. 6: Rozdělení metodiky analýzy rizik [60]

### 3.2.1 Vybrané základní metody analýzy rizik

Níže vyčtené metody pro analýzu rizik byly vytvořeny pro konkrétní, specifický záměr a zaměření problému, tudíž nejsou vzájemně porovnatelné. Naopak je při analyzování rizik vhodné jednotlivé metody kombinovat. Také je nutno na metody pohlížet pouze jako na pomocný nástroj, lidská inteligence zůstává hlavní složkou. Níže popsané metody jsou v souladu se zveřejněnými metodami Ministerstva vnitra ČR. [65]



- Kontrolní seznam – Check List (CL)

Tato metoda využívá již existující kontrolní seznamy a porovnává je s praxí. Metodu je možné použít v různých fázích vývoje organizace, včetně fáze projektování ve smyslu kontroly souladu se standardními podmínkami. Pokud je nevyhnutelné vytvářet nový kontrolní seznam, musí analytik využít informace z příslušných právních a odborných norem a předpisů. Často bývá kombinovaná s jinými metodami jako je například What-If analýza.

- Analýza toho, co se stane když – What If Analysis (WI)

Analýza „Co se stane, když...“ je často využívanou metodou, jejíž podstata je založená na brainstormingu, při kterém se analytický tým snaží identifikovat možná rizika na základě pokládání přímých otázek. Účinnost této metody se váže ke schopnosti dodržování pravidel brainstormingu, velikosti analytického týmu, vztahu k organizaci apod.

- Bezpečnostní kontrola – Safety Audit (SA)

Manažerský nástroj skládající se ze systematické periodické a objektivní evaluace bezpečnosti organizace, managementu a nástrojů s cílem pomoci zabezpečit aktiva systému prostřednictvím manažerské kontroly bezpečnosti, zdraví a environmentálních praktik s hodnocením dodržování zavedených standardů. Bezpečnostní audit může být realizovaný u všech typů subjektů, včetně veřejné správy.

Pravidelně opakující se bezpečnostní audit zabezpečí úspěšnost managementu rizik v systému. Vzhledem ke své univerzálnosti patří tato metoda k nejstarším. Bezpečnostní audit je nejčastěji realizovaný ve třech etapách. První etapou je samotná příprava na bezpečnostní audit, ve druhém kroku probíhá realizace auditu a poslední krok náleží výstupu proběhlého auditu v podobě dokumentací jako například auditní správa, která obsahuje popis a zhodnocení celkového stavu bezpečnosti, seznam nejzávažnějších zjištění a posouzení závažnosti vyplývajících rizik jednotlivého zjištění a hodnocení stavu závěrečných bezpečnostních opatření. V závěru je vykonaná prezentace výsledků s vhodnými návrhy opatření.

- Předběžná analýza ohrožení – Preliminary Hazard Analysis (PHA)

PHA metodika se obvykle využívá pro vytvoření seznamu veškerých nebezpečí v blízkém okolí objektu a využívá se pro poskytnutí přehledu ohrožení v krátkém časovém intervalu, který je následně použit pro detailní analýzu. Základní myšlenkou této analýzy je zvolení předmětu a identifikovat problémy, které by mohly působením vlivu vzniknout.

- Analýza nebezpečí a provozuschopnosti – Hazard Operation Process (HAZOP)

Jedním z nejjednodušších a také nejrozšířenějších přístupů k identifikaci nebezpečí je samotné studium nebezpečí a provozuschopnosti. Analýza byla vyvinuta společností ICI-Petrochemicals Division ve Velké Británii a v současné době představuje uznávaný standard při posuzování nebezpečí a zajišťování bezpečnosti složitých chemických zařízení. Ve značné míře je analýza využívána v chemickém průmyslu pro posouzení nových projektů a při rekonstrukci provozu organizace.

- Analýza stromu událostí – Event Tree Analysis (ETA)

Jedná se o graficko-statickou metodu, při níž je vytvářen systémový strom událostí, který je reprezentován rozvětveným grafem s dohodnutou symbolikou a popisem. Rozvětvený graf stromu událostí sleduje průběh procesů od iniciační události přes konstruování událostí z hlediska příznivosti a nepříznivosti. Znárodnuje veškeré události s jistou mírou výskytu. Rozvětvenost grafu závisí na počtu jednotlivých událostí.

- Analýza příčin poruch a jejich následků – Failure Mode and Effect Analysis (FMEA)

Pomocí této metody je možné sestavit tabulku příčin, poruch a jejich promítnutí na funkčnosti systému. Identifikuje jednoduché poruchy, které mohou přispět k vážnější havárii. Výsledkem je kvalitativní, systematický seznam jednotlivých subsystémů, jejich poruch a následek s možností kvantifikace.

- Analýza stromu poruch – Fault Tree Analysis (FTA)

Podstatou této metody je deduktivní hledání jednotlivých rizik a určování jejich příčin. Jedná se o grafický model kombinací různých rizik a chyb člověka, které mohou vyústit do tzv. „vrcholové události“. Hlavním cílem této metody je posouzení pravděpodobnosti vrcholové události s využitím analytických nebo statistických metod. Metoda byla původně vyvinuta pro potřeby technických operací a poté našla široké uplatnění v jaderné energetice. Právě na základě své spolehlivosti se její využití velmi široké – je aplikovatelná na všechny druhy technických a technologických rizik. Její nevýhodou je časová náročnost a potřebné zkušenosti analytického týmu.

- Analýza spolehlivosti člověka – Human Reliability Analysis (HRA)

Systematické hodnocení faktorů, které determinují činnost jednotlivých osob v organizaci, se nazývá metoda analýzy lidského faktoru. Cílem této metody je analyzovat potenciální lidské selhání, chyby, jejich příčiny a následek. Podstatou této metody je získání informací

o činnosti organizace o podmínkách, ve kterém realizují svou činnost ve spojení s celkovou připraveností lidí. Systematicky vyjmenovává chyby, které se mohou vyskytnout během provozu. Metoda často využívá spojení s jinými metodami jako například FTA. Informace jsou pro potřeby analýzy získávány z interních dokumentací organizace, rozhovory s lidmi a anketováním.

- Analýza stromu nebezpečí – Hazard Tree Analysis (HTA)

Základním a zásadním prvkem pro sestavení stromu nebezpečí je volba typu havárie, která je postačující na pokrytí problémů, které máme zájem řešit. Jednotlivé typy havárií jsou roztrženy na počátku vytváření analýzy. Při tomto roztržení je nutné, aby se dané podtřídy typu havárie vzájemně vylučovaly, aby byly na každé úrovni obdobně vyznačeny a měly úplný logický dosah působnosti

- Relativní hodnocení – Relative Ranking (RR)

Relativní hodnocení je posuzování nebezpečnosti procesu na základě chemicko-fyzikálních vlastností látek, technickobezpečnostních parametrů, jejich množství a dalších charakteristických jevů. Tato metoda neumožňuje sledování souvislostí příčin a následku. K tomuto typu metod se řadí například: Dowův index hořlavosti a výbušnosti, Mondův index, Index nebezpečnosti látky a Index působení chemických vlivů. Jejich výhodou je velmi rychlý způsob klasifikace potenciálního nebezpečí v organizaci.

- Analýza příčin a následků – Causes and Consequences Analysis (CCA)

Tato metoda je spojením metod ETA a FTA. Využívá se jako komunikační nástroj, jehož diagram vyjadřuje vztahy mezi následky rizik a jejich základními příčinami. Metoda analýzy příčin a následků se využívá v jednoduchých případech mimořádných událostí, spojuje výsledky obou analýz do jednoho diagramu. Výsledkem je popis potenciálních rizik, přičemž je v diagramu. Možné sledovat rizikové sekvence a scénáře.

- Analýza hrozeb a rizik pro měkké cíle – Soft Targets Analysis (STA)

Metodika je určena zejména vedoucím pracovníkům a provozovatelům měkkých cílů, kteří jsou v pozici o rozhodování rozvoje bezpečnostního systému. Konkrétně výsledky analýzy slouží nejen bezpečnostním profesionálům, ale i managementu dané společnosti pro potřeby posouzení jednotlivých nabídek dodavatelů a pro podporu v rozhodování pro jednu z několika cest bezpečnosti podniku nebo jiného měkkého cíle. Výsledkem analýzy není přesně

vypočítaná číselná tabulka, vypracována na podkladě matematických vzorců. Jde o jednoduchý, ale velmi účelně zaměřený myšlenkový proces, který napomůže k porozumění možných hrozeb. [53, 60, 65]

### 3.2.2 Indexové metody

Mimo základní metodiky pro vytvoření analýzy rizik jsou dostupné také některé metody, jejichž podstata je v porovnání jednotlivých specifických indexů.

- Threshold Planning Quantity Index (TPQ)

Metoda byla vyvinuta organizací Environmental Protection Agency a zaměřuje se na kontrolu obsažení látek a sledování překročení jejich limitů.

- Rapid Ranking (RR)

Jako jedna z nejnovějších metod dané oblasti nám umožní hodnocení nebezpečí díky zahrnutí indexu hořlavosti a výbušnosti, které se stanovují na základě materiálního faktoru míry tzv. všeobecného a specifického nebezpečí v procesu. Dále se pak zabývá toxicitou a jejím indexem, který vychází z faktoru nebezpečí poškození zdraví v úměrnosti výskytu a koncentrace dané nebezpečné látky. Metoda se využívá hlavně ve Spojených státech.

- Chemical Exposure Index (CEI)

Metoda vytvořená společností Dow's Chemical Company, využívána pro posuzování ohrožení toxickými látkami.

- Dow's Fire and Explosion Index (F&EI)

Metoda vznikla pod křídly společností Dow's Chemical Company pro identifikaci nebezpečí požáru a výbuchu procesních jednotek. F&EI uvažuje rozmanité faktory, jakými jsou například látkové vlastnosti, procesní podmínky apod.

- Material Hazard Index (MHI)

Metoda byla vyvinuta pro posouzení a stanovení limitních stavů nebezpečných látek v oblasti bezpečnosti, kdy hraniční hodnoty musí být zabezpečeny bezpečnostním opatřením.

- Substance Hazard Index (SHI)

Metoda byla navržena organizací Organization Resources Counselors jako nástroj pro klasifikaci úrovně nebezpečných látek. Samotný index SHI symbolizuje podíl rovnoměrně vyskytující se koncentrace látky za normální teploty a prudce toxické koncentrace totožné látky ve vzduchu. [50, 60]

### 3.3 Bezpečnostní opatření pro minimalizování rizik

Pro případ prevence neboli předcházení rizik, je v současné době běžnou součástí moderních organizací a firem propracovaná bezpečnostní politika, která v dlouhodobém hledisku při správném aplikování a dodržování plnění, přispívá k výraznému snížení míry bezpečnostních rizik.

- Fyzická bezpečnosti

Fyzická bezpečnost se sestává ze základních technických dokumentací, které jsou účelně navrhnuté pro zabezpečení fyzické bezpečnosti konkrétního referenčního objektu. Mezi dokumenty fyzické bezpečnosti patří:

- Směrnice fyzické bezpečnosti,
- Mechanické a zábranné systémy,
- Poplachové zabezpečovací a tísňové systémy,
- Kamerové systémy,
- Přístupové systémy. [66]

- Režimová opatření

Režimová opatření zaznamenávají způsoby ochrany, kterými by se měli zaměstnanci a členové dané organizace řídit v rámci preventivní ochrany. Definují se v nich režimy, které je nutno dodržovat v jednotlivých strukturách a funkcích organizace. Definice organizačních režimových opatření musí být v souladu s lidskými právy a svobody a jakákoliv omezení musí být v souladu s platnými zákony (například BOZP a PO).

Režim je definovaný jako organizační, administrativní a věcné uspořádání vztahů mezi lidmi v interním a externím prostředí organizace a jejich činnostmi a procesy v oblasti výkonu a řízení, za účelem sdílení veškerých prvků s cílem dosažení harmonického stavu v daném referenčním objektu. Pod režimová opatření spadá:

- Činnost zaměstnanců v interním prostředí podniku,

- Pohyb a chování cizích osob v objektu,
- Výstup interních informací do externího prostředí. [67]
- Bezpečnostní dokumentace

Bezpečnostní dokumentací se stanovují konkrétní pravidla v rámci bezpečností politiky organizace, která jsou následně nutná dodržovat všemi vrstvami struktury. Interní legislativa organizace patří k optimálnímu způsobu pro prosazení stanovených cílů. Jednotlivé dokumenty jsou v organizaci uvedeny jako interní směrnice, nařízení, pokyny, pracovní postupy a funkční popisy. V případě definování uvedených dokumentů, musí dojít ke stanovení kompetencí neboli určení povinnosti a zodpovědnosti konkrétních zaměstnanců. Tato kompetence může spadat na interní pracovníky nebo se může využít forma tzv. outsourcingu<sup>2</sup>. Dokumenty musí obsahovat jednotlivé body v postupu pro předejití před riziky:

- Specifikace a popis činnosti,
- Jmenování zodpovědné osoby pro danou činnost,
- Časový harmonogram/provedení dané činnosti,
- Způsob správného provedení činnosti. [66]
- Krizové řízení

Krizové řízení se využívá organizací při události bezpečnostního incidentu, kdy je potřebné mít sestavený funkční tým odborníků, který v čase případné náhlé události převezme vedení a aplikuje krizový plán. Tento tým musí pravidelně absolvovat jednání a aktualizovat bezpečnostní plán pro potřeby organizace v krizi. [68]

- Školení

Mezi podstatné prvky bezpečnostního opatření patří pravidelné školení zaměstnanců v jednotlivých vrstvách struktury organizace. Při školení dochází k obeznámení členů s interními směrnici, jejich novelami a formou vhodného aplikování do praxe. Proces školení se řadí mezi nedůležitější složku v bezpečnostním opatření jakékoliv organizace, jelikož je v samotném důsledku za plněním daných směrnic a vytvořených opatření lidský faktor. Vzhledem k tomuto faktu se musí klást velký důraz na dodržování tohoto procesu.

---

<sup>2</sup> Outsourcing – využívání externí společnosti pro zajištění dílčího procesu v organizaci. [69]

### Dílčí závěr

Analýza rizik vědecky prognózuje budoucí projevy a důsledky bezpečnostních hrozeb, které se opírají o získaná objektivní fakta. Principy využitých metodik pro analýzu rizik se od sebe velmi odlišují a mají svá specifika. Proto je vhodné pro adekvátní analýzu využít více než jednu metodiku.

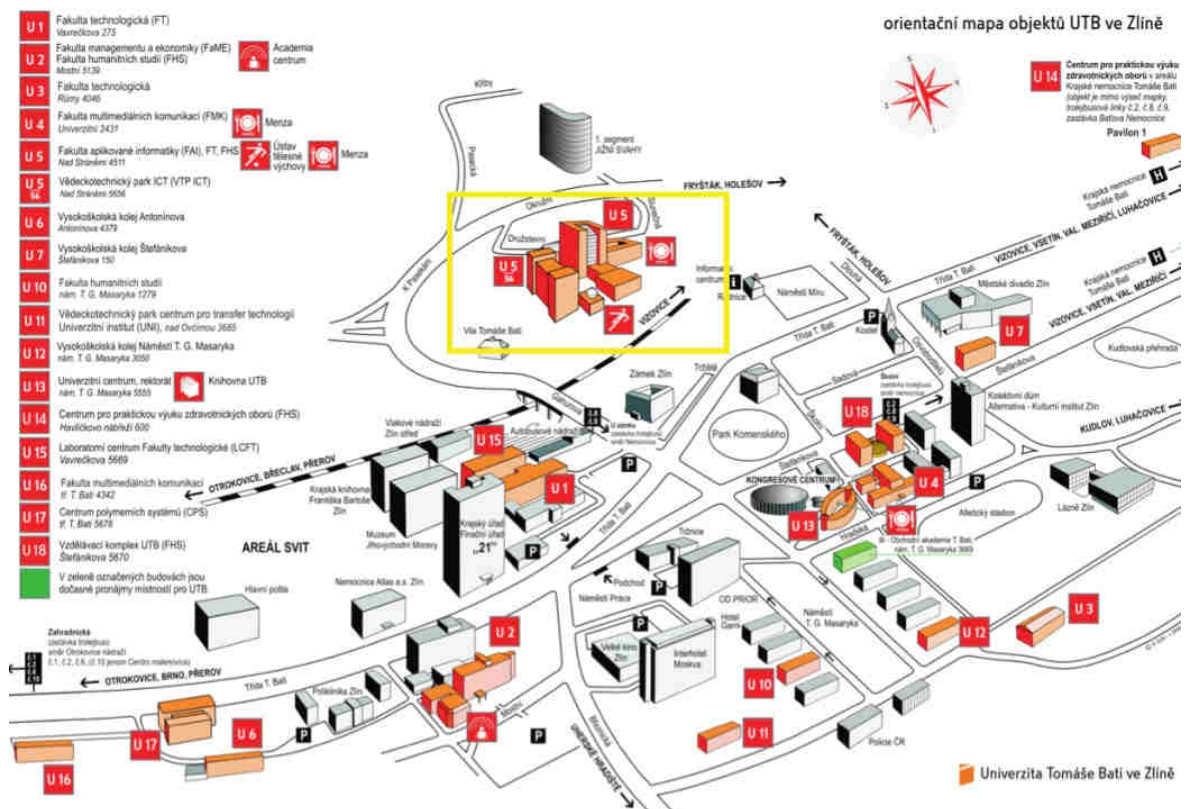
Výběr vhodné metodiky se podvoluje konkrétnímu záměru, se kterým je analýza rizik tvořena. Například metoda Event Tree Analysis je známá pro svou přehlednost a srozumitelné grafické znázornění, naproti tomu je analýza What-If, jejímž výstupem je psaný text – seznam otázek a odpovědí. Analýza Failure Mode and Effects Analysis vyhodnocuje míru rizika závažnosti, odhalení a pravděpodobnosti, zatímco metoda Soft Targets Analysis klade důraz na analyzování mimo jiné i načasování a umístění potenciální hrozby.

## **II. PRAKTICKÁ ČÁST**



## 4 FAKULTA APLIKOVANÉ INFORMATIKY UTB

Fakulta aplikované informatiky (FAI) Univerzity Tomáše Bati (UTB) je jedna z šesti fakult zlínské UTB. Byla založena k datu 1. ledna 2006 oddělením se od Institutu řízení procesů a aplikované informatiky, kdy vznikla samostatná FAI v městské části Jižních svahů, na adrese: Nad Stráněmi 4511, 760 05, Zlín, Česká republika. Na obrázku (Obr. 7) je možné vidět umístění Fakulty aplikované informatiky v rámci celého univerzitního komplexu UTB ve Zlíně. [70]



Obr. 7: Umístění budovy U5 ve Zlíně [70]

### 4.1 Lokace a okolí objektu

Referenční objekt je umístěn severně od centra města Zlín, v části zvané Jižní svahy, na místě, kde se dříve nacházela 13. Základní škola a nenachází se v blízkém okolí průmyslové či komerční oblasti. Jižní svahy se vyznačují množstvím bytových panelových domů s velmi hustou obydleností – až čtvrtina celkového počtu občanů města Zlín (76 000 obyvatel) žije právě v této městské části. [71] Kromě řady panelových domů, kterými je fakulta obklopena, se v blízkém okolí nachází další objekty:

- Vědeckotechnický park Informační a komunikační technologie

VTP-ICT je propojen se samotným referenčním objektem proskleným tunelem, ve kterém je průchod podmíněn čipovou kartou. V objektu se nachází 40 kanceláří, 8 laboratoří spolu s jednacími a seminárními místnostmi. V budově sídlí nad dvacet společností, k největším patří například PRIA SYSTEM s.r.o., Edhouse, s.r.o., Business Logic, s.r.o., a jiné firmy, zabývající se vývojem a správou informačních a komunikačních technologií. V tabulce (Tab. 4) je konkretizovaná otevírací doba VTP-ICT. [70]

Tab. 4: Otevírací doba VTP-ICT [70]

Otevírací doba	
Po-Pá	06:00-22:00
So-Ne	zavřeno

- Bytové domy

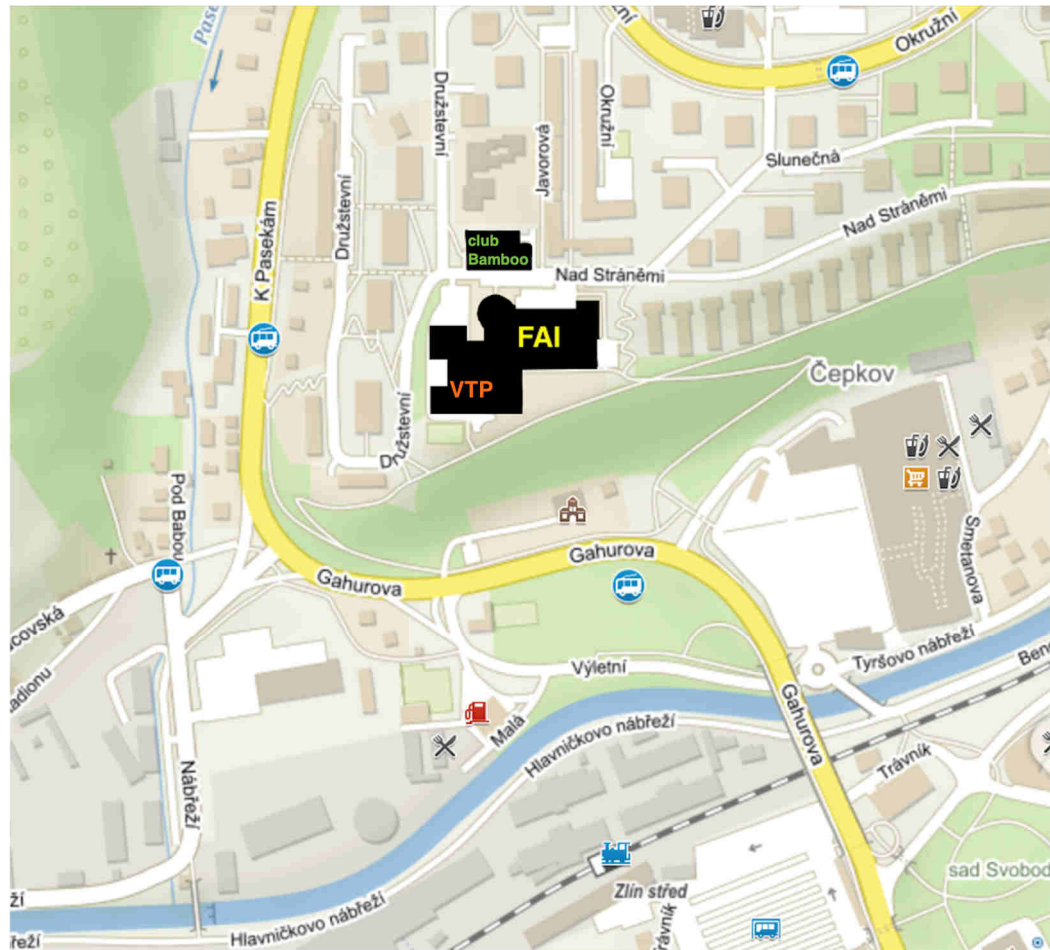
V blízkém okolí fakulty se nachází desítky bytových domů, které mají v průměru 4 poschodí a průměrně 5 bytů na patře. Jedná se tak o stovky bytů, jejichž majitelé mohou jednotlivé byty nabízet k pronájmu. Evidence reálných osob, využívajících prostor bytů, mohou být těžce dohledatelné a verifikovatelné. Osoby tak mohou být různého věku, národnosti, vyznání, aj. a jejich pohyb a činnosti jsou zcela neřízené.

- Bamboo club

Bamboo club je karibská restaurace a bar, který několikrát do týdne funguje v noci jako klub. Nabízí také možnost pronájmu prostor pro soukromé oslavy, promítání filmů, pořádání živých koncertů a jiných speciálních akcí. V níže přiložené tabulce (Tab. 5) je zaznamenaná otevírací doba Bamboo clubu a obrázek znázorňuje dislokaci vyjmenovaných objektů pro jasné znázornění. [72]

Tab. 5: Otevírací doba Bamboo club [72]

Otevírací doba	
Út-Pá	16:00-22:00
So	16:00-02:00
Ne-Po	zavřeno

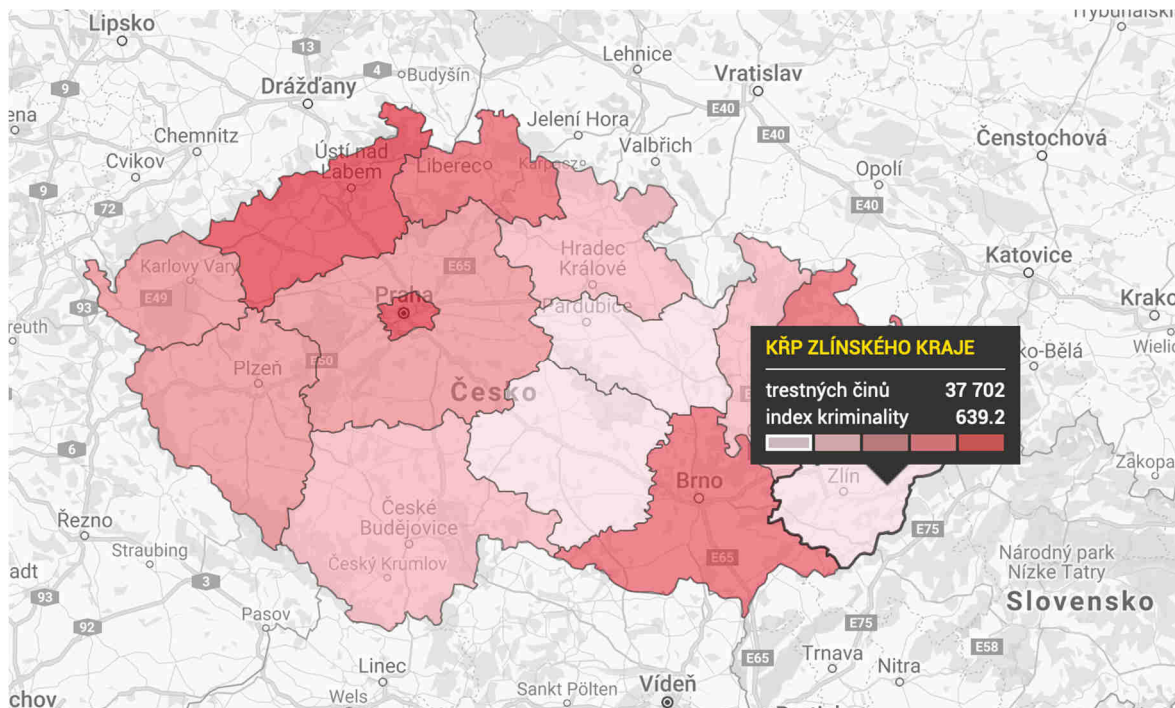


Obr. 8: Dislokace FAI, VTP-ICT a Bamboo klubu ve Zlíně [73]

## 4.2 Kriminalita

Město Zlín se neřadí mezi kriminálně významná města. I přesto, že se v něm nachází mnoho krajských institucí, kulturních památek a sportovišť, je v kontextu celé České republiky město Zlín méně vyhledávané kriminálními zločinci. Proto samotné riziko teroristického útoku je v tomto městě malé.

Dle mapy kriminality, graficky znázorněné na obrázku (Obr. 9), došlo ve Zlínském kraji za posledních 5 let (od února roku 2014) k 37 702 trestným činům a je tak v pořadí třetím krajem s nejmenším počtem trestních činů v České republice. [74]



Obr. 9: Mapa kriminality Zlínského kraje [74]

V rámci kraje je samotný Zlín městem s nejvyšším počtem spáchaných trestných činů, což je dáno zejména tím, že jde o největší město v kraji. V indexu kriminality je však Zlín až na druhém místě po městu Vsetín.

V tomto ohledu je riziko spáchání trestného činu v rámci Zlínského kraje velké, ale v porovnání s obdobně velkými městy, (jak je možno vidět v Tab. 6) v České republice je index kriminality poměrně malý. Například index kriminality města Most dvojnásobně převyšuje index města Zlín, i přesto, že má Zlín více obyvatel. [74]

Tab. 6: Porovnání zlínské trestné činnosti s městy s podobným počtem obyvatel [74]

Město	Počet obyvatel	Index kriminality
Pardubice	90000	804
Zlín	76000	625
Havířov	72000	1300
Kladno	69000	1017
Most	67000	1384

### 4.3 Složky Integrovaného záchranného systému

V případě, že by došlo k nějaké formě teroristického útoku v referenčním objektu, je zapotřebí zjistit, jak dlouho by trval dojezd jednotlivým složkám IZS města Zlín a tudíž, jak rychle by se dostalo pomoci postiženým lidem uvnitř nebo v blízkosti objektu.

Zdravotnická záchranná služba:

- Peroutkovo nábřeží 434, dojezdový čas 10 minut,
- L. Váchy 602, dojezdový čas 11 minut.

Hasičský záchranný sbor:

- Profesionální: Přílucká 213, dojezdový čas 9 minut,
- Dobrovolný: Švermova 103, dojezdový čas 11 minut.

Policie ČR:

- Krajské ředitelství: J. A. Bati 5637, dojezdový čas 7 minut,
- Územní odbor: nám. T. G. Masaryka, dojezdový čas 6 minut,
- Obvodní oddělení: tř. T. Bati 44, dojezdový čas 8 minut.

Městská policie Zlín:

- Služebna Okružní 4699, dojezdový čas 1 minuta,
- Služebna Santražiny 3312, dojezdový čas 7 minut. [75]

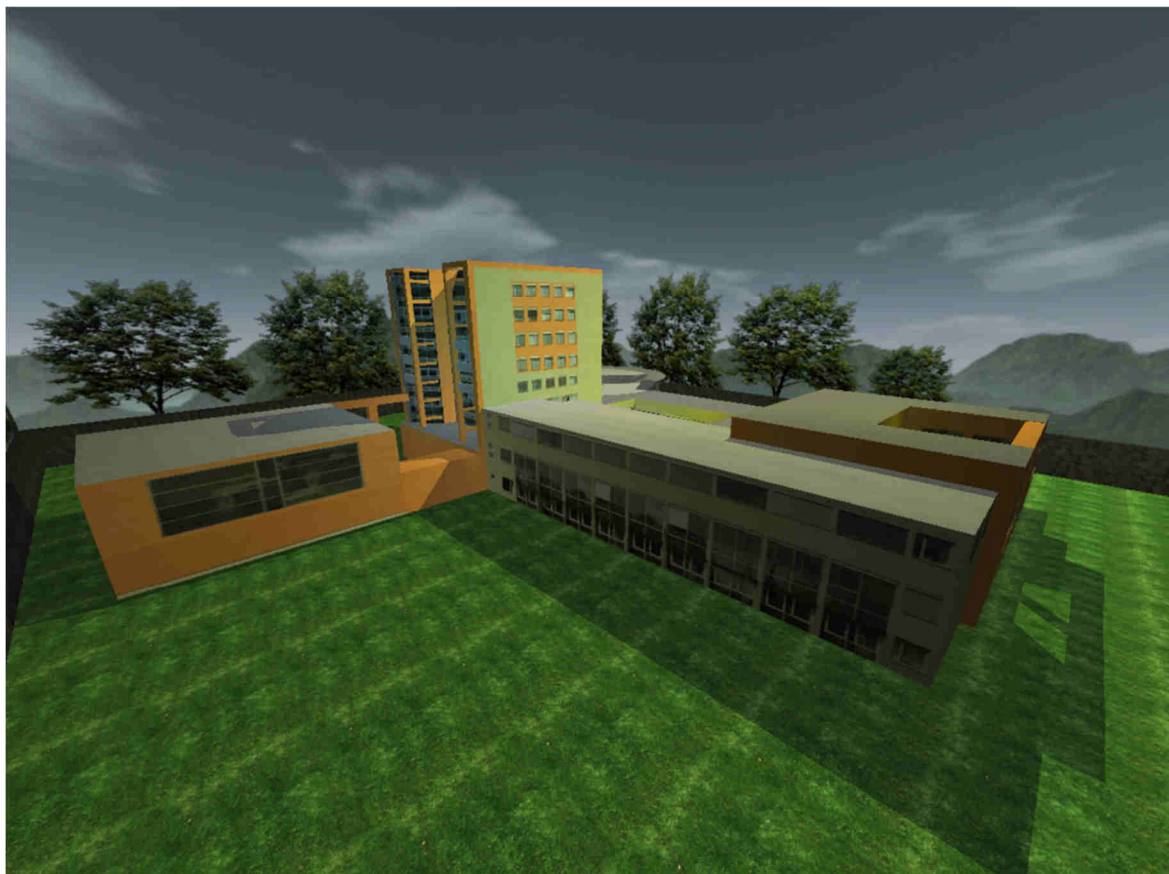
Dojezd všech složek IZS k Fakultě aplikované informatiky je možný do 11 minut. Nejbližše se nachází služebna Městské policie Zlín, kde by jednotky za optimálních podmínek dokázaly příjezd do referenčního objektu do jedné minuty.

Avšak hustý provoz v centru města Zlín zejména v ranních hodinách (kolem osmé hodiny) a v odpoledních hodinách (kolem páté hodiny) by mohl zkomplikovat příjezd každé jednotlivé složky Integrovaného záchranného systému ke komplexu FAI.



#### 4.4 Popis referenčního objektu

Komplex FAI je složen z jednotlivých pavilonů, jejíž nosná, střešní a stropní konstrukce je z nehořlavého, železobetonového skeletu. Jednotlivé pavilony jsou navzájem propojeny a celek referenčního objektu je tak stupňovitý s rovnými střechami (Obr. 10). Jednotlivé pavilony fakulty se tedy různí v počtu podlaží. Západní pavilon (U51), nejvyšší část objektu, má osm pater.

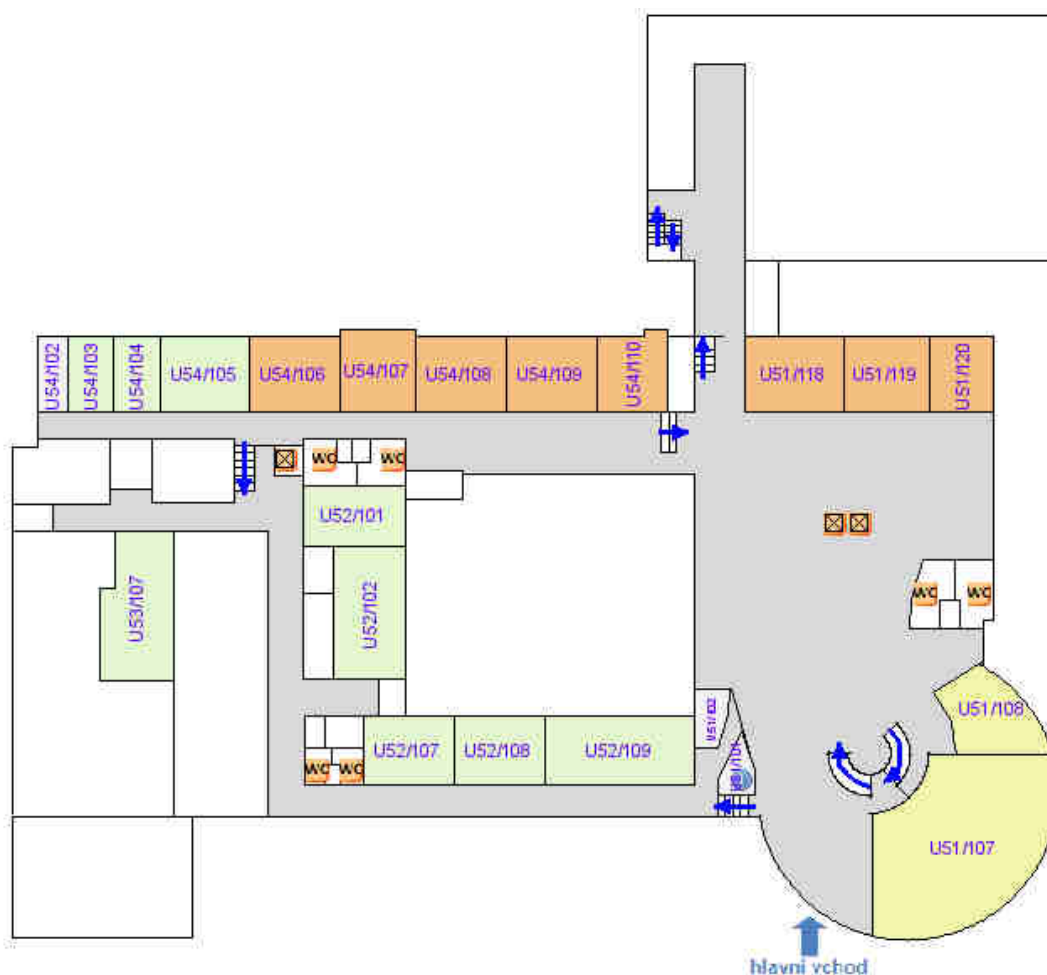


*Obr. 10: Fakulta aplikované informatiky ve Zlíně [76]*

Dostupnost do každého patra je možná po schodišti anebo jedním ze dvou výtahů. Další částí komplexu je severní pavilon (U52), který má pouze dvě poschodí, východní úsek (U53) se třemi poschodími, jižní část (U54) také se třemi poschodími a poslední úsek U55, ve kterém sídlí tělocvična, je jednopodlažní. Referenční objekt je otevřen denně od 06:00 do 22:00 hod. a největší kumulace osob v objektu je mezi 09:00 a 15:00, kdy probíhá většina přednášek, seminářů a vědeckých činností. Po celou dobu je objekt střežen outsourcingovou fyzickou ostrahou společnosti SG'3. Bezpečnostní společnost SG'3 ve Zlíně působí již 19 let a má centrálu na adrese: nám. T. G. Masaryka 588, 760 01 Zlín. [70, 77]

- První podlaží budovy U5

Ihned po vstupu do budovy se na východní straně budovy nachází prosklená buňka s fyzickou ostrahou, která přicházejícím návštěvám slouží také pro poskytnutí potřebných informací. Naproti fyzické ostrahy je nejprostornější přednášková místnost v referenčním objektu (U51/107) s kapacitou pro 161 osob. Mimo tuto místnost jsou v prvním patře necelé dvě desítky menších místností s kapacitou 12–36 osob určené pro vzdělávací/pedagogickou činnost, opatřené vstupem na čipovou kartu. Dále se nachází v prvním patře pánské a dámské sociální zařízení a množství volně uspořádaných stolů se židlemi ve foyer. Pro představu rozložení prvního patra slouží obrázek (Obr. 11). [77]



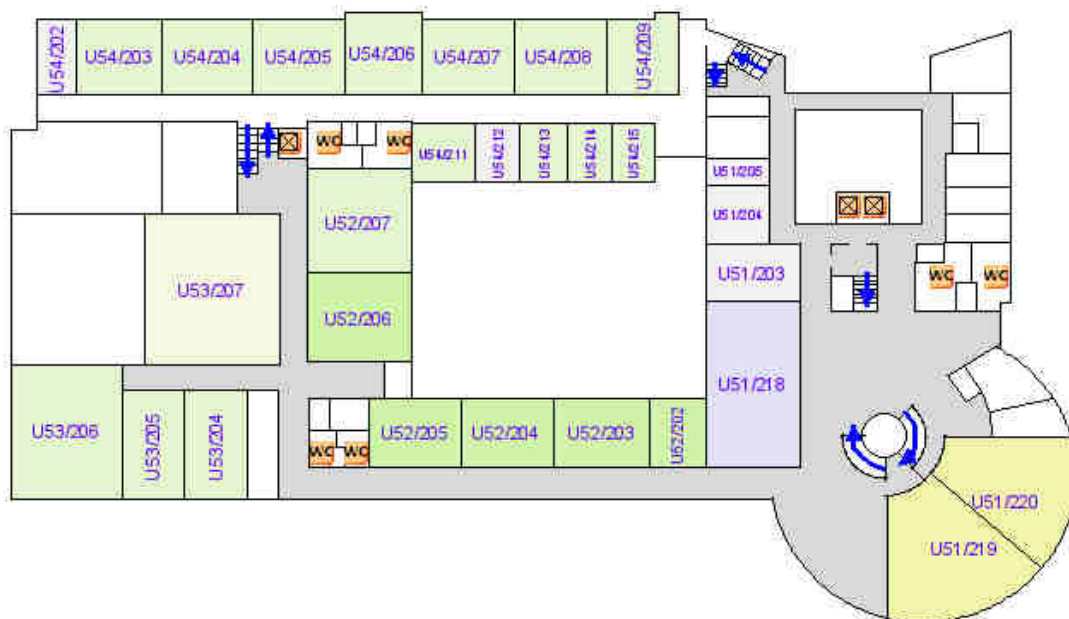
Obr. 11: První podlaží budovy U5 [77]

- Druhé podlaží budovy U5

Pro vstup do druhého podlaží lze využít točitého schodiště u hlavního vstupu do objektu, jednoho z prosklených výtahů ve foyer (v pavilonu U51) anebo zvolit variantu schodů či výtahu (v úseku U53). Nejprostornějšími místnostmi ve druhém patře je posluchárna

U51/219 s kapacitou pro 88 osob, posluchárna U51/220 pro 60 osob a studovna, která pojme 44 osob. Studovna s počítači má omezenou otevírací dobu: Po – Pá od 08:00 do 18:00.

Dále se na podlaží nachází patnáct menších laboratoří s kapacitou 12 osob, pět počítačových učeben s kapacitou 10–24 osob, stravovací zařízení, které má kapacitu na pojetí 64 osob v otevírací době: Po – Pá od 7:30 do 15:00 a oddělené sociální zařízení, vyznačené na níže přiloženém plánu druhého podlaží na obrázku (Obr. 12). [70, 77]

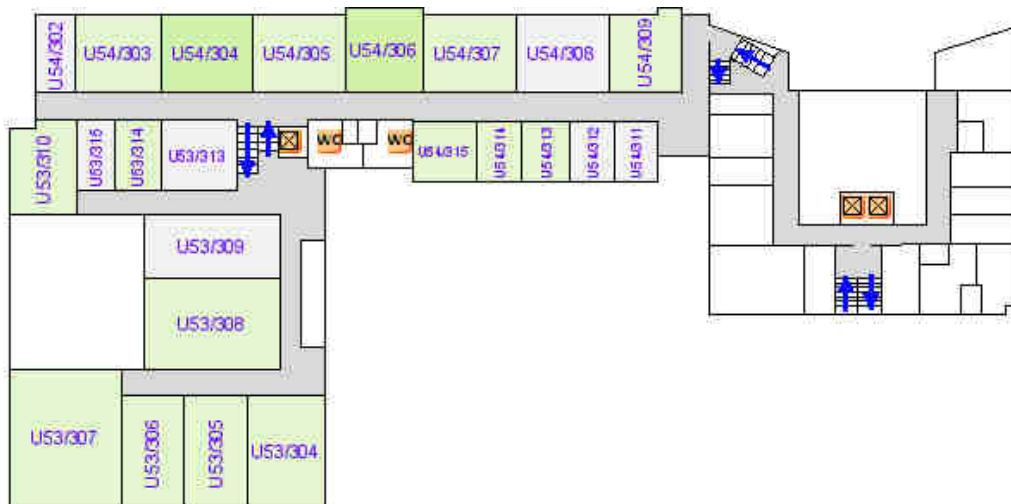


Obr. 12: Druhé podlaží budovy U5 [77]

- Třetí podlaží budovy U5

Obrázek (Obr. 13) představuje jižní a východní pavilon (U53 a U54) třetího podlaží, který je určen zejména pro vědecko-výzkumnou činnost. Konkrétně ve třetím patře kromě sociálních zařízení nalezneme čtrnáct laboratoří s průměrnou kapacitou 15 osob, dvě počítačové učebny s kapacitou 12 a 24 osob a desítku menších místností sloužící k nespécifikovaným účelům. Západní pavilon (U51) referenčního objektu je vyhrazen pro kanceláře zaměstnanců fakulty s kuchyňkou a sociálním zařízením na každém jednom patře. [70, 77]



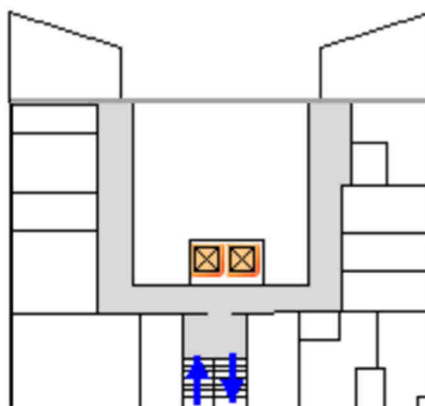


Obr. 13: Třetí podlaží budovy U5 [77]

- Čtvrté až osmé podlaží budovy U5

Tím, že je komplex FAI stupňovitý, do výšky čtvrtého až osmého patra spadá pouze západní pavilon (U51), ve kterém se nachází pracovní pro zaměstnance fakulty. Konkrétně jsou patra rozdělena podle zaměření, ale prostorově zůstávají neměnná (viz Obr. 14). Každé jedno patro je vybaveno kuchyňkou a sociálním zařízením.

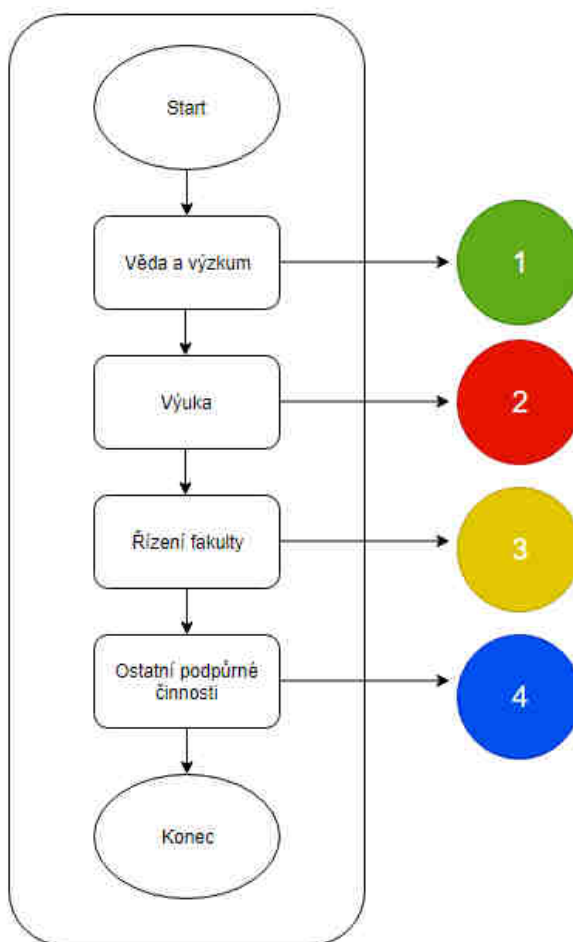
Čtvrté patro je vymezeno jako zázemí pro firmy, které s fakultou spolupracují. V pátém patře sídlí Ústav informatiky a umělé inteligence spolu s Ústavem řízení procesů. V šestém patře se nachází děkanát a tajemník fakulty, oddělení tvůrčích činností, oddělení zahraničních vztahů a propagace, oddělení pro spolupráci s praxí, technické oddělení, ekonomické oddělení a zasedací místnost. Sedmé patro náleží Ústavu bezpečnostního inženýrství a Ústavu automatizace a řídicí techniky. V posledním, osmém patře, sídlí Ústav počítačových a komunikačních systémů a Ústav elektroniky a měření. [70, 77]



Obr. 14: Čtvrté až osmé podlaží budovy U5 [77]

## 4.5 Procesy objektu

V níže přiloženém diagramu na obrázku (Obr. 15), jsou znázorněny a vzestupně seřazeny procesy objektu FAI, podle významnosti pro fakultu. Mezi hlavní procesy se tedy řadí proces výuka a věda a výzkum spolu s potřebnými a neméně důležitými průvodními procesy, jakými je organizace a řízení fakulty a další podpůrné činnosti. [70]



Obr. 15: Hlavní procesy objektu [zdroj: vlastní]

- Věda a výzkum

Proces věda a výzkum začíná specifikováním druhu a záměru projektu, po kterém se vyhodnotí pole poptávky a nabídky. Následuje pohyblivá složka ve formě získání dotací a grantů. Poté nastává samotná realizace stanoveného projektu, kdy těsně před nebo po jeho dokončení probíhá zhodnocení výstupu projektu s celkovým vyhodnocením projektu (viz. Obr. 16). [70]



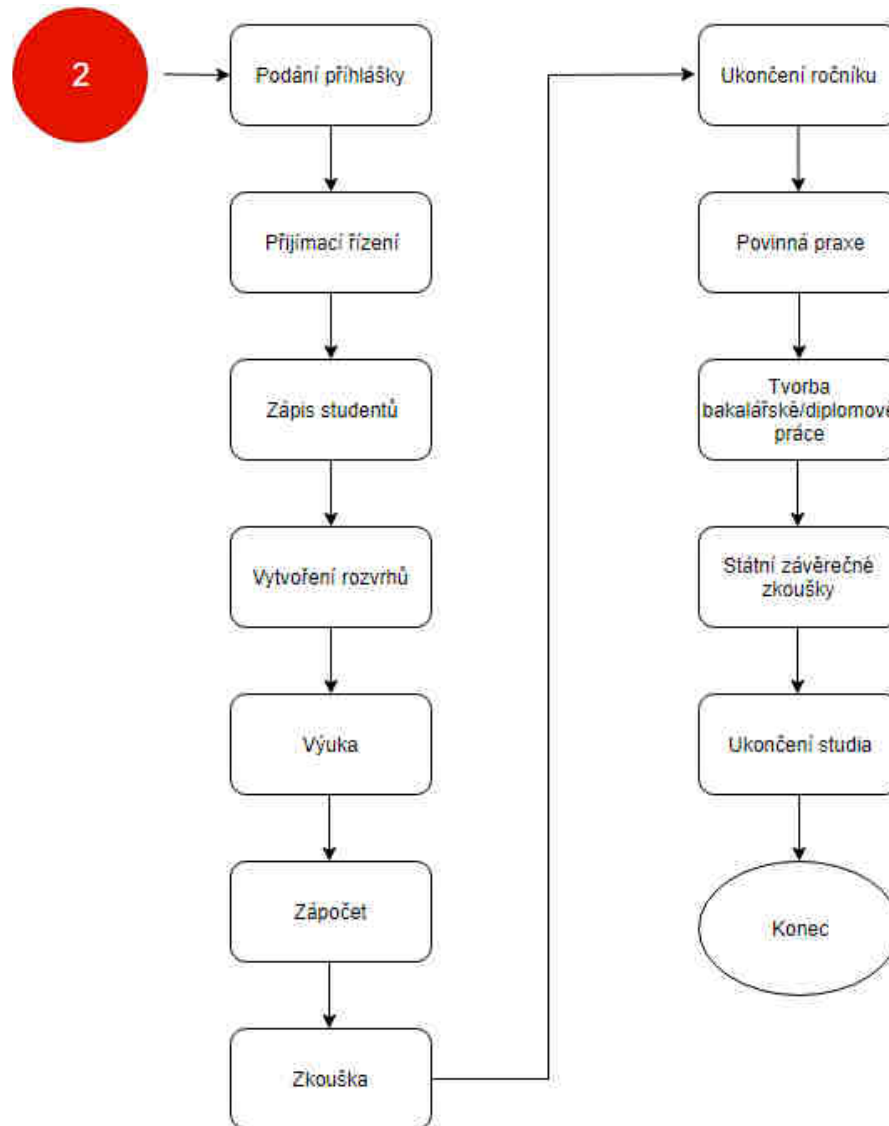
Obr. 16: Věda a výzkum[zdroj: vlastní]

- Výuka

Proces výuky, který v sobě odráží šíření znalostí a pedagogickou činnost začíná samotnou aktivitou ze strany studenta, který se rozhodne podat přihlášku na FAI (viz diagram na Obr. 17). Po tomto kroku dochází k přijímacímu řízení, které se v dnešním stavu koná u vybraných studijních oborů. Následně se uskuteční zápis studentů, při kterém se do databáze zavádí údaje o studentech, která se promítají do informačního systému fakulty. Na základě těchto dat v systému, může být vytvořen rozvrh pro jednotlivé ročníky a obory, díky kterým může být prováděna výuka.

Po ukončení výuky dochází k ukončení předmětu, což zpravidla splněním zápočtu a dosažení minimálního počtu bodů pro složení zkoušky daného předmětu. Tím dochází ke splnění předmětů a následně ukončení ročníku. V prezenční formě studia je třeba splnit

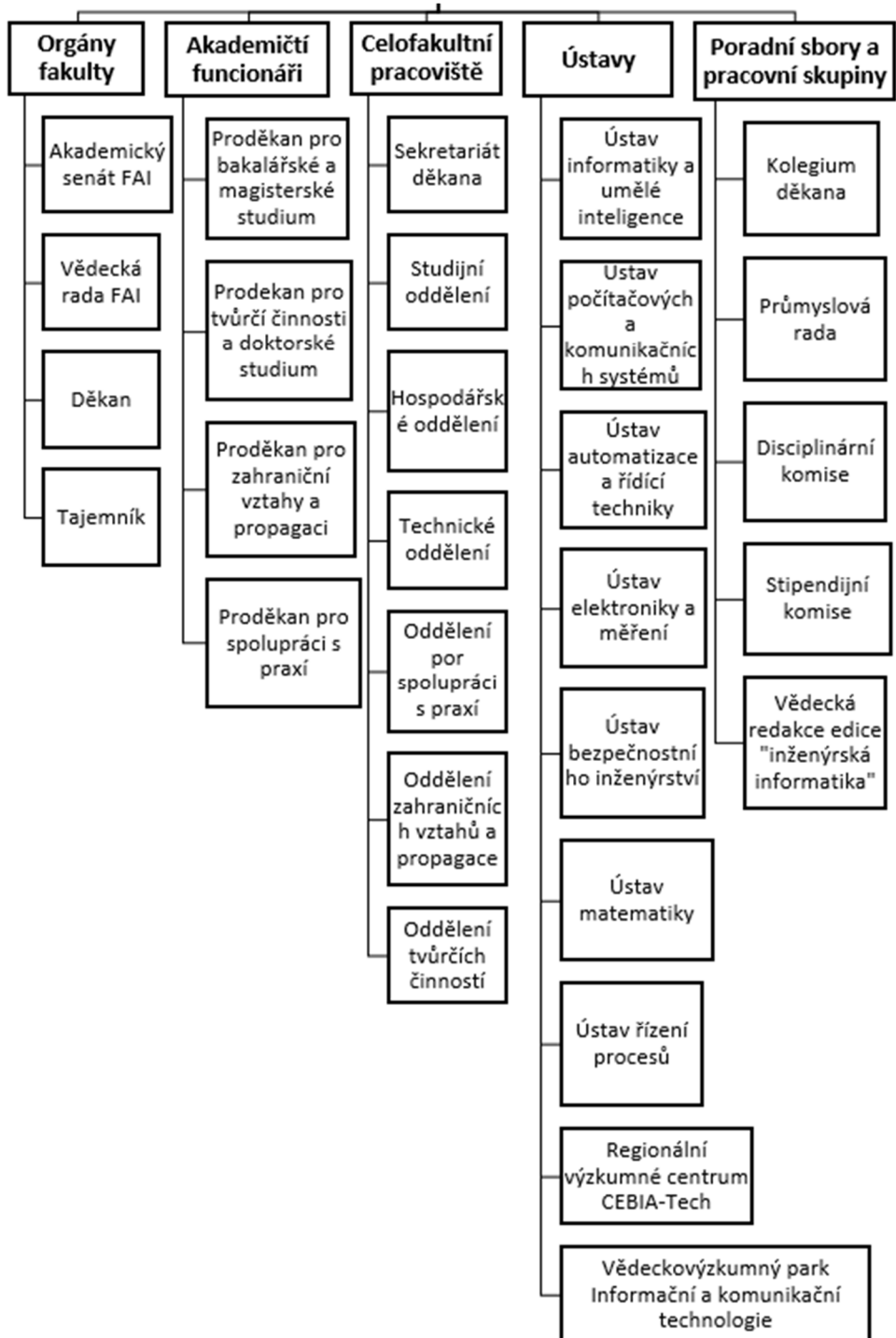
povinnou praxi. Po úspěšném splnění všech předmětů, doložením splněním povinné praxe a vytvořením bakalářské/diplomové práce, se proces výuka završí státní závěrečnou zkouškou a následným ukončením studia. [70]



Obr. 17: Výuka [zdroj: vlastní]

- Řízení fakulty

Proces řízení fakulty (Obr. 18) reflektuje členitou organizační architekturu, která rozděluje působení mezi jednotlivé orgány fakulty, ke kterým patří například Akademický senát FAI, Disciplinární komise, Vědecká rada FAI a děkan s tajemnicí. Dále si rozdělují moc jednotliví akademičtí funkcionáři, konkrétní ústavy FAI a pracovní skupiny, které představuje například stipendijní komise, skládající se ze členů akademických pracovníků a studentů. Jednotliví členové mohou plnit v rozvětvené struktuře fakulty více rolí. [70]

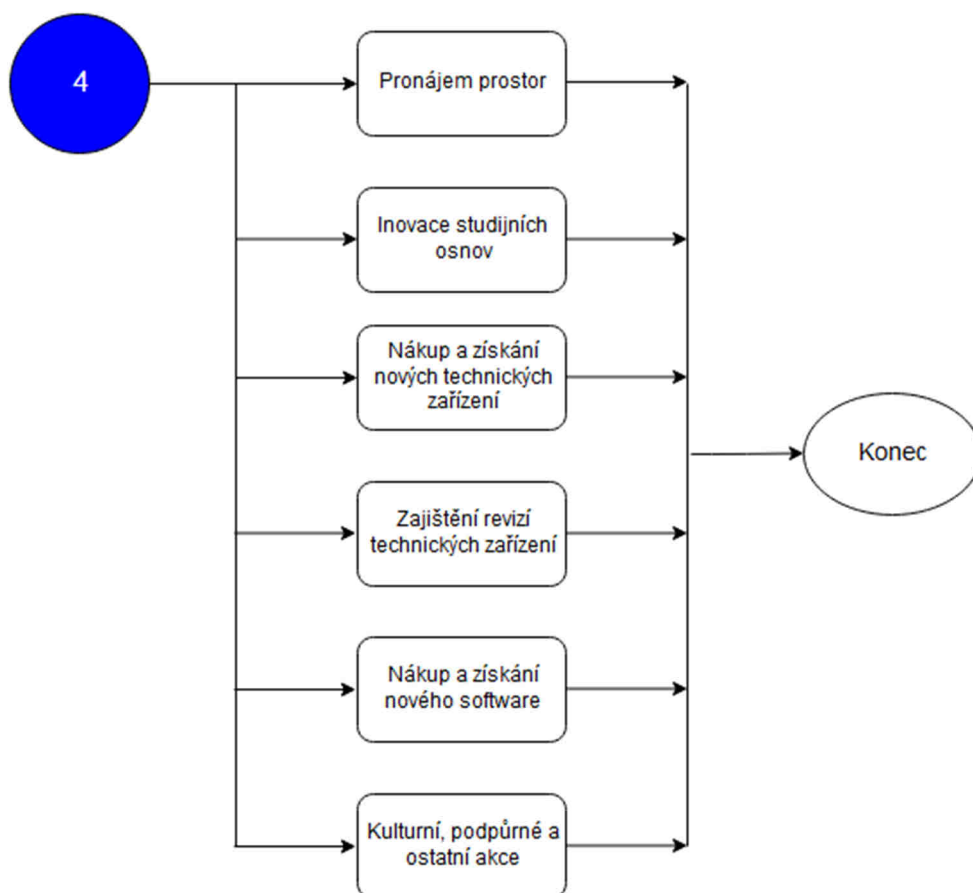


Obr. 18: Řízení fakulty [70]

- Ostatní podpůrné činnosti

Mezi další procesy fakulty patří procesy podpůrné, které slouží v zásadě pro rozvoj aktivit a zkušeností studentů a akademických pracovníků. Řadí se zde kulturní a podpůrné akce, kterými jsou například pravidelně pořádané Robogames nebo Noc vědců, které spojují s prostředím fakulty i potenciální uchazeče o studium, dále pak Studentská tvůrčí a odborná činnost (STOČ), které se mohou účastnit státnicové ročníky z řad studentů.

V rámci fakulty jsou umožněny výjezdy do zahraničí na různě dlouhá časová období pro studenty i akademické pracovníky. Fakulta také propůjčuje své prostory pro konání nejrůznějších konferencí, workshopů, veletrhů a mimo jiné i část svých prostor dlouhodobě pronajímá firmám. Mimo další podpůrné činnosti patří například inovace studijních osnov, nákup a získání nových technických zařízení, nákup a získání nového software a zajištění revizí technických zařízení. Pro přehled ostatních podpůrných činností fakulty slouží obrázek (Obr. 19). [70, 77]



Obr. 19: Ostatní podpůrné činnosti [zdroj: vlastní]

## 4.6 Identifikace aktiv

Cílem určení aktiv je stanovení předmětu ochrany z hlediska bezpečnosti prostředí FAI ve Zlíně. Pro tento účel je třeba vymezit aktiva, která mají z pohledu ochrany měkkých cílů hlavní prioritu a je potřeba je adekvátně chránit. Mezi nejvýznamnější aktivum FAI proto patří veškeré osoby, pohybující se uvnitř budovy. Jsou jimi:

### a) Studenti bakalářského stupně studia

Bakalářský stupeň vzdělání na FAI je tříleté a probíhá v pěti různých oborech v českém jazyce v rámci studijního programu Inženýrská informatika. Pro zájemce studia Informačních a řídicích technologií je umožněno studium celého bloku i v jazyce anglickém. V prezenční formě celkově studuje 515 studentů (viz. Tab. 7), kombinovanou formu navštěvuje 238 studentů a dlouhodobých zahraničních studentů bakalářského stupně studia jsou dva. [78]

Tab. 7: Studenti prezenční, anglické a kombinované formy bakalářského studia [78]

BAKALÁŘSKÉ STUDIUM	Prezenční forma	Kombinovaná forma	Anglický jazyk
Bezpečnostní technologie, systémy a management	140	112	x
Informační a řídicí technologie	80	105	x
Informační technologie v administrativě	120	x	x
Inteligentní systémy s roboty	30	21	x
Softwarové inženýrství	145	x	x
Information and Control Technologies	x	x	2

### b) Studenti magisterského stupně studia

Dvouleté magisterské studium se realizuje v šesti oborech v českém jazyce a ve dvou oborech v jazyce anglickém. Z nich má největší zastoupení studentů konkrétně obor Bezpečnostní technologie, systémy a management v kombinované i prezenční formě (viz. Tab. 8). Celkově je počet studentů v magisterském studiu ve všech formách 372. [78]

Tab. 8: Studenti prezenční, anglické a kombinované formy magisterského studia [78]

MAGISTERSKÉ STUDIUM	Prezenční forma	Kombinovaná forma	Anglický jazyk
Automatické řízení a informatika	3	7	x
Bezpečnostní technologie, systémy a management	36	177	x
Informační technologie	26	93	x
Integrované systémy v budovách	3	x	x
Počítačové a komunikační systémy	16	14	x
Učitelství informatiky pro střední školy	23	x	x
Security Technologies, Systems and Management	x	x	3
Information Technologies	x	x	7
Integrated Systems in Buildings	x	x	2

## c) Studenti doktorského stupně vzdělání

FAI nabízí dva čtyřleté obory, které jsou umožněny studovat v českém i anglickém jazyce, v prezenční i kombinované formě. V aktuálním roce pojímají všechny formy doktorského studijního programu 112 studentů. Podrobnější popis se nabízí v tabulce (Tab. 9). [78]

Tab. 9: Studenti prezenční, anglické a kombinované formy bakalářského studia [78]

DOKTORSKÉ STUDIUM	Prezenční forma	Kombinovaná forma	Anglický jazyk
Inženýrská informatika	24	64	x
Automatické řízení a informatika	3	12	x
Engineering Informatics	x	x	8
Automatic Control and Informatics	x	x	1

## d) Krátkodobí zahraniční studenti

Je zapotřebí také zmínit specifickou skupinu studentů, kteří díky množství bilaterálních smluv, které FAI v rámci mezinárodního programu Erasmus+ a Freemover nabízí, mohou po vymezené období studovat a navštěvovat na půdě fakulty.



V uplynulém zimním semestru roku 2018/2019 bylo na fakultě přijato 27 zahraničních studentů, konkrétně ze zemí: Francie, Turecko, Rusko, Řecko, Španělsko, Itálie, Litva, Polsko a Kazachstán. Největší početní zastoupení měli studenti z Turecka, kterých bylo na fakultě více než polovina z celého počtu krátkodobých studentů v daném období.

Nynější, letní semestr, oproti předešlému hostuje také studenty z Tchaj-wanu, Ukrajiny, Portugalska, Indonésie a Gruzie, s největším poměrem zastoupení studentů z Ruské federace. Celkový počet zahraničních studentů programu Erasmus+ v letním semestru školního roku 2018/2019 je 35. [78]

e) Akademičtí pracovníci

K roku 2019 FAI zaměstnává 131 pracovníků. Konkrétně se jedná od 41 odborných asistentů, 42 technicko-hospodářských pracovníků a jiné pozice, popsané v tabulce (Tab. 10).

*Tab. 10: Konkrétní pozice a počet akademických pracovníků na FAI v roce 2019 [78]*

Pozice	Počet
Profesor	7
Docent	15
Odborný asistent	41
Asistent	9
Lektor	2
TH pracovník	42
Výzkumník	15

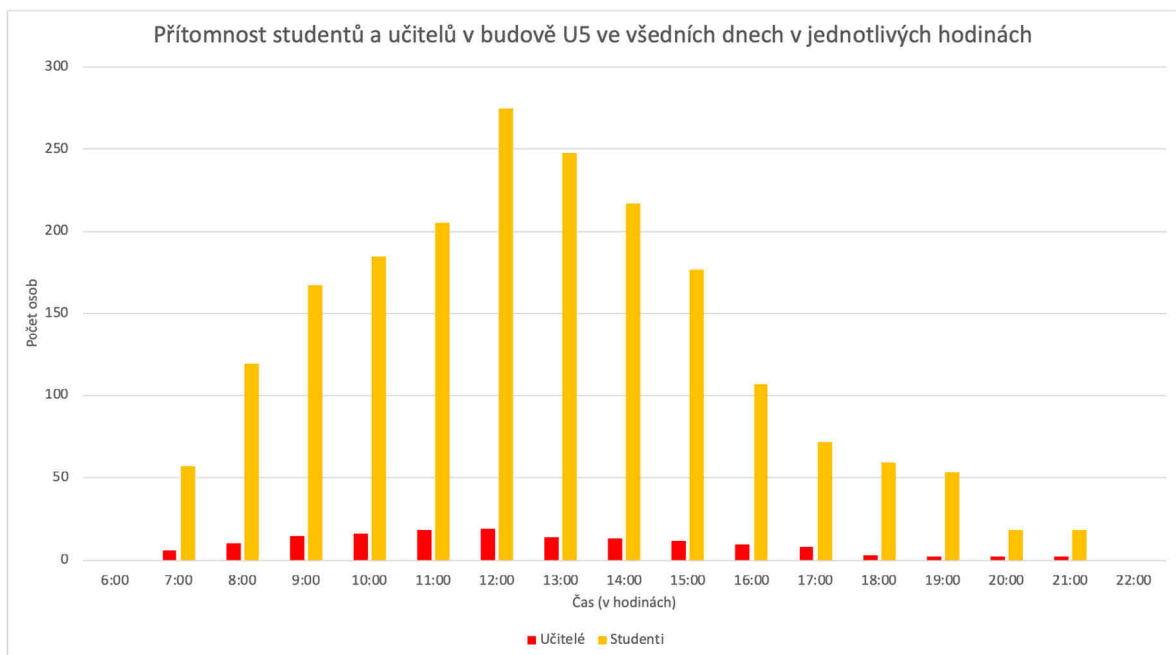
- f) Návštěvy v objektu budovy U5,
- g) Pronajímatelé jednotlivých prostor v komplexu fakulty,
- h) Lidé využívající pronajímané prostory v komplexu fakulty.

#### 4.7 Návštěvnost referenčního objektu

Návštěvnost v referenčním objektu se významně liší v závislosti na harmonogramu akademického roku. Níže vyobrazený graf (Obr. 20) zaznamenává odhadovanou průměrnou návštěvnost studentů a učitelů na FAI v letním semestru ve všedních dnech, v rámci povinných aktivit zaznamenaných informačním systémem STAG. Údaje vycházejí z databáze informačního systému za období 4. 2. 2019 – 10. 5. 2019. [78]

V rámci grafu nejsou zahrnuty pohyblivé složky, jako například účast studentů a učitelů na jednorázových akcích (Robogames, STOČ, promoce atd.), aktivity v tělocvičně, zkouškové termíny a také graf počítá s nulovou absencí ve výuce. Také zde není brán ohled na faktor volného opuštění prostor referenčního objektu.

Z grafu vyplývá, že největší koncentrace osob v budově U5 je mezi 9:00 a 15:00. Přítomnost studentů se změní ve zkouškovém období, které trvá 5 týdnů v zimním semestru a 4 týdny v semestru letním. V období mezi 22:00 a 06:00 je budova uzavřena a celý referenční objekt je hlídán fyzickou ochranou poskytovanou bezpečnostní společností SG'3. [70, 78, 79]



Obr. 20: Průměrná přítomnost studentů a učitelů v budově U5 ve všedních dnech letního semestru akademického roku 2018/ 2019 [78, 79]

## 4.8 Bezpečnostní opatření

Jak již bylo zmíněno, systém fyzické bezpečnosti je řešen fyzickou ostrahou, která je najímána bezpečnostní společností SG'3. Pracovní náplní ostrahy je nepřetržitý dohled nad budovou, k čemuž ostraze dopomáhá integrované dohledové centrum s výstupy z kamerových zařízení umístěných v referenčním objektu a kamer, dohlížejících na okolí objektu. Mimo svou hlavní náplň ostraha přichází do kontaktu s činnostmi, jakými je například evidence a vydávání klíčů jednotlivých místností a učeben, poskytování informací, třídění pošty anebo zaznamenávání závad. Fyzická ostraha má dvousměnný provoz, s čímž se také váží rozdíl-

nosti jednotlivých směn. Referenční objekt je otevřen do 22 hodin, avšak dohled nad objektem a jeho okolím probíhá i po uzavření budovy. V níže přiložené tabulce (Tab. 11) je zobrazen výčet skupin osob s oprávněným a řízeným vstupem a jejich charakteristikou.

Ostraha denního provozu má v popisu práce:

- Podávat informace,
- Obsluhovat elektrické jističe, hl. uzávěry, aj.,
- Evidovat návštěvy,
- Vydávat přístupové karty a klíče od učeben a místností,
- Řešit dopravní situace v těsné blízkosti objektu,
- Obsluhovat protipožární, kamerový a zabezpečovací systém,
- Přijímat poštovní zásilky,
- Předávat a uchovávat informace a věci.

Ostraha nočního provozu má v popisu práce:

- Kontrolovat těsné okolí budovy,
- Uchovávat a vydávat věci,
- Provádět doplňkové práce,
- Kontrolovat omezení přístupnosti,
- Kontrolovat prostory referenčního objektu,
- Evidovat osoby v objektu po ukončení.

Systém technické ochrany je realizován pomocí prvků PZTS, EPS a CCTV a ACS. V každé přednáškové a seminární místnosti jsou umístěny PIR detektory. Jedná se o všechny patra do 3. podlaží (včetně) a obecně jsou detektory v každé místnosti, která má okna. Poté je na každém patře jeden PIR detektor s dlouhým dosahem. Při vstupních dveřích jsou umístěny kamery a vchodové dveře jsou opatřeny magnetickými kontakty, napojenými na EPS. Dále se v učebnách nachází opticko-kouřové hlásiče, sirény a tísňová tlačítka.

Co se týče systému kontroly vstupu, je proveden formou čteček karet na vybraných místech uvnitř budovy a tzv. klíčovou službou za pomoci participace fyzické ostrahy, která má v popisu práce vydávání klíčů osobám s povolením. V následující tabulce (Tab. 11) jsou popsány dílčí charakteristiky skupin osob vyskytujících se v referenčním objektu s oprávněným a řízeným vstupem.

Tab. 11: Charakteristika osob s oprávněným a řízeným vstupem v objektu U5 [70,78]

Skupina osob	Charakteristika
<b>Osoby s oprávněným vstupem</b>	
Prezenční studenti	<ul style="list-style-type: none"> <li>- Oprávnění ke vstupu je podmíněno zápisem ke studiu</li> <li>- Návštěvnost je každodenní v rámci výuky</li> <li>- Věková hranice skupiny 19–31 let</li> </ul>
Kombinovaní studenti	<ul style="list-style-type: none"> <li>- Oprávnění ke vstupu je podmíněno zápisem ke studiu</li> <li>- Návštěvnost je nepravidelná a velmi omezená</li> <li>- Věková hranice 19 - neomezeně</li> </ul>
Akademičtí pracovníci	<ul style="list-style-type: none"> <li>- Oprávnění ke vstupu podmíněno pracovní smlouvou</li> <li>- Jednotlivé úlohy definované pracovní smlouvou</li> <li>- Návštěvnost je každodenní, definovaná pracovní časem</li> <li>- Věková hranice 18- neomezeně</li> <li>- Povinnost proškolení interních směrnic, BOZP a Požární ochrany</li> </ul>
Technicko-hospodářští zaměstnanci	<ul style="list-style-type: none"> <li>- Oprávnění ke vstupu a přítomnost v objektu přesně definovaná pracovní smlouvou s referenčním objektem anebo zprostředkovaně (outsourcing)</li> <li>- Požadavky a doba trvání činnosti v rámci referenčního objektu definovaná pracovní smlouvou</li> </ul>
Úlohoví externí zaměstnanci	<ul style="list-style-type: none"> <li>- Ke konkrétní specifikaci docházky dochází v pracovní smlouvě</li> <li>- Přítomnost v objektu je přesně definovaná</li> </ul>
<b>Osoby s řízeným vstupem</b>	
Uchazeči o studium	<ul style="list-style-type: none"> <li>- Návštěvnost je nárazová</li> <li>- Pohyb a případné činnosti jsou pod dohledem</li> <li>- Věková hranice 18 – 19</li> </ul>
Zástupci firem pro spolupráci	<ul style="list-style-type: none"> <li>- Nelze definovat intervaly návštěv</li> <li>- Nelze specifikovat věk</li> <li>- Možnost zavedení politiky přístupu s protokolem nahlašování kategorií návštěv</li> </ul>
Nájemníci prostor	<ul style="list-style-type: none"> <li>- Nelze definovat intervaly vstupu</li> <li>- Nelze specifikovat věk návštěvníků</li> <li>- Možnost zavedení oprávnění ke vstupu částečně řízeno nájemní smlouvou</li> </ul>
Zákazníci nájemníků prostor	<ul style="list-style-type: none"> <li>- Nelze definovat věk</li> <li>- Řízení vstupu podléhá nastavení pravidel daného nájemce</li> <li>- Zodpovědnost za zákazníky přebírá nájemce</li> </ul>
Návštěvy	<ul style="list-style-type: none"> <li>- Zcela neuchopitelná skupina osob</li> <li>- Nelze definovat věk</li> <li>- Nelze definovat intervaly přístupu</li> <li>- Možnost zavedení přístupového systému</li> </ul>

### Dílčí závěr

Fakulta aplikované informatiky je situována v městské části Jižní svahy, kde sídlí od roku 2006. V její blízkosti se nachází VTP-ICT, Bamboo club a řada bytových domů. Kriminalita města Zlín v porovnání s ostatními městy s obdobným počtem obyvatel je poměrně malá. K referenčnímu objektu jsou schopny, v případě nutnosti (a optimálních podmínek) veškeré složky IZS, dojet do času 11 minut.

Fakulta se skládá z několika pavilonů, které jsou navzájem propojeny a tvoří tak stupňovitý komplex. Každé patro objektu je specifické svou funkcí a osobami, jenž se v něm pohybují. Mezi hlavní procesy fakulty patří věda a výzkum, výuka, řízení fakulty a ostatní podpůrné činnosti, ke kterým patří například pořádání veletrhů, konferencí apod.

Osoby, pohybující se uvnitř budovy, neboli aktivum fakulty, se dělí do skupin jako například: studenti (bakalářského, magisterského, doktorského stupně vzdělání), akademičtí pracovníci, návštěvy, pronajímatelé prostor v budově FAI a lidé, využívající těchto pronajímaných prostor. Návštěvnost se v průběhu roku velmi odlišuje v návaznosti na harmonogram akademického roku a daných akcích, konaných fakultou.

## 5 FMEA ANALÝZA

V závislosti na zveřejněné metodice Ministerstva vnitra České republiky – Základy ochrany měkkých cílů, obsahujícím seznam četnosti a typologie nejčastějších násilných útoků na měkké cíle, byl vytvořen seznam 10 nejčastějších násilných útoků a tedy podklad, sloužící pro výčet potencionálních hrozeb referenčního objektu Fakulty aplikované informatiky a následném analyzování metodou analýzy možných příčin a jejich důsledků.

Tabulka (Tab. 12) obsahuje klasifikaci závažnosti (Z) a její kritéria, ohodnocující závažnost problému. Vzhledem k charakteru aktivům referenčního objektu, jsou kritéria závažnosti specifikována na ohrožení zdraví a života osob, vyskytujících se v objektu a jeho těsné blízkosti.

Tab. 12: Klasifikace závažnosti [zdroj: vlastní]

Míra závažnosti	Kritéria závažnosti	Bodové ohodnocení
Velmi vysoká	Smrt skupiny osob	10
	Smrt jednotlivce	9
	Těžký úraz více osob	8
Vysoká	Těžký úraz jedné osoby	7
	Lehký úraz více osob	6
Střední	Lehký úraz jedné osoby	5
	Malý úraz více osob	4
Nízká	Úraz jedné osoby	3
	Mírné poškození zdraví	2
Žádná	Bez poškození zdraví	1

Klasifikace pravděpodobnosti odhalení (O) v tabulce (Tab. 13), řeší míru odhalení možné hrozby, kdy míra odhalení „neodhalitelné“ zastává formu, kdy riziko není možné odhalit před samotným vznikem nežádoucí události. Dalšími úrovněmi jsou těžce odhalitelné, středně odhalitelné, lehce odhalitelné a zjevné, kdy s klesající mírou odhalení klesá také pravděpodobnost včasného zásahu.

Tab. 13: Klasifikace odhalení [zdroj: vlastní]

Míra odhalení	Pravděpodobnost odhalení	Bodové ohodnocení
Neodhalitelné	Nemožná detekce	10
	Nepravděpodobná detekce	9
	Velmi nízká pravděpodobnost detekce	8
Těžce odhalitelné	Nízká pravděpodobnost detekce	7
	Střední pravděpodobnost detekce	6
Středně odhalitelné	Poloviční pravděpodobnost detekce	5
	Vysoká pravděpodobnost detekce	4
Lehce odhalitelné	Velmi vysoká pravděpodobnost vysoká	3
	Téměř vždy odhalitelná	2
Zjevné	Vždy odhalitelná	1

Četnost výskytu ( $P$ ), rozčleněná dle pravděpodobnosti na velmi vysokou, vysokou, střední, malou a zanedbatelnou, kdy se k nejméně častým řadí událost, která nastane v řádech desítek let a za událost s velmi vysokým výskytem se považuje jev, který nastane několikrát za den. Stanovené ohodnocení dle četnosti výskytu je vystihnuto tabulkou (Tab. 14).

Tab. 14: Klasifikace výskytu [zdroj: vlastní]

Pravděpodobnost výskytu	Četnost výskytu	Ohodnocení
Velmi vysoká	1x za den	10
	1x za týden	9
	1x za 2 týdny	8
Vysoká	1x za měsíc	7
	1x za 3 měsíce	6
Střední	1x za 6 měsíců	5
	1x za rok	4
Malá	1x za 5 let	3
	1x za 10 let	2
Zanedbatelná	1x za 50 let	1

Tabulka (Tab. 14) zaznamenává proces výpočtu míry rizika. S tím, že hranice přijatelnosti rizika pro referenční objekt dle expertního posouzení stanovila na hodnotu 200 (20 %), kdy pod tuto hodnotu spadají rizika, jejichž míra rizikovosti je podmíněčně přijatelná či přijatelná, a naopak hodnoty vyšší, než je stanovená hranice, spadají pod tzv. nepřijatelná rizika a v tabulce jsou znázorněna červeně.

Tab. 15: FMEA referenčního objektu [29]

P. č.	Hrozba	P	O	Z	Míra rizika	Výsledek
1	Napadení chladnou zbraní	4	8	3	96	OK
2	Napadení střelnou zbraní	4	7	8	224	NOK
3	Žhářský útok	4	4	6	96	OK
4	Braní rukojmí a barikádová situace	3	7	2	42	OK
5	Výbušnina v poštovní zásilce	2	4	9	72	OK
6	Sebevražedný útok s použitím výbušniny	2	6	10	240	NOK
7	Výbušnina v zaparkovaném vozidle	3	9	9	243	NOK
8	Nájezd vozidla s výbušninou se sebevražedným útočником	2	6	8	108	OK
9	Útok nájezdem vozidla	2	6	3	36	OK
10	Útok s použitím výbušniny (bez přítomnosti útočníka)	4	9	10	360	NOK

Násobkem pravděpodobnosti výskytu, odhalení a závažnosti, vyjde v analýze míra rizika, která se dle výše uvedené mezní hodnoty 200, rozdělí na míru přijatelného (OK) a míru nepřijatelného (NOK) rizika pro referenční objekt.

Jak lze v tabulce (Tab. 15) vidět, červené hodnoty patří do skupiny rizik nepřijatelných a je tedy potřebné stanovit patřičná bezpečnostní opatření, vhodná pro podmínky referenčního objektu. Jako nejrizikovější je tedy konkrétně hrozba útočníka s použitím výbušniny bez jeho přítomnosti. Můžeme si tedy představit útočníka, který projde vstupem do objektu se zavazadlem v libovolné velikosti, obsahujícím výbušninu, které uvnitř budovy ponechá a k samotnému výbuchu dojde po opuštění místa činu útočníkem.

V pořadí druhou nejrizikovější hrozbou je dle analýzy FMEA výbušnina, ponechaná v zaparkovaném vozidle v těsné blízkosti objektu. Dalším rizikem v pořadí, je sebevražedný útok s použitím výbušniny. Chápáno jako útočník, na kterém je umístěna výbušnina, projde vstupem do objektu a po dohledání určitého cíle, odpálí výbušninu. Posledním hrozbou



s hodnotou míry rizika nad 200, je napadení útočnicka střelnou zbraní, kde hlavním problémem opět nastává samotný vstup útočnicka do objektu. Tabulka (Tab. 16) reflektuje příčinu a nastavuje vhodné trvalé opatření, po jehož zavedení se jeho účinek následně promítne v podobě snížení míry rizika pod stanovenou mezní hodnotu.

Tab. 16: FMEA analýza s náležitým opatřením a mírou rizika po aplikování trvalého opatření [zdroj: vlastní]

P.č.	Hrozba	Míra rizika	Výsledek	Okamžité opatření	Kořenová příčina	Trvalé opatření	Míra rizika po opatření
10	Útok s použitím výbušniny (bez přítomnosti útočnicka)	360	NOK	detekování výbušniny ostrahou, evakuace objektu a kontaktování policie.	nedostatečná kontrola vstupujících osob	rotační turniket se systémem kontroly vstupu	160
7	Výbušnina v zaparkovaném vozidle	243	NOK	detekování podezřelého vozidla a kontaktování policie	nedostatečný zábranný systém, možnost parkování v těsné blízkosti objektu	betonové zábrany	108
6	Sebevražedný útok s použitím výbušniny	240	NOK	zadržení pachatele a evakuace objektu	nedostatečná kontrola vstupujících osob	rotační turniket se systémem kontroly vstupu	80
2	Napadení střelnou zbraní	224	NOK	zakročení ostrahy a předání útočnicka policii	nedostatečná kontrola vstupujících osob	rotační turniket se systémem kontroly vstupu	128
3	Žhářský útok	235	OK				
1	Napadení chladnou zbraní	216	OK				
8	Nájezd vozidla s výbušninou se sebevražedným útočnickem	162	OK				
5	Výbušnina v poštovní zásilce	144	OK				
4	Braní rukojmí a barikádová situace	98	OK				
9	Útok nájezdem vozidla	24	OK				

### Dílčí závěr

V rámci FMEA analýzy byly vytyčeny jednotlivé klasifikace závažnosti, odhalení a výskytu, jejichž bodové ohodnocení je nedílnou součástí pro stanovení míry rizika jednotlivých hrozeb. Seznam hrozeb byl inspirován Ministerstvem vnitra České republiky, konkrétně ze Základu ochrany měkkých cílů Ing. Zdeňka Kalvacha. Následně se jednotlivé útoky hodnotily dle specifických klasifikací a tím se určila míra rizika.

Dále byla stanovena mezní hranice míry rizika, která tak rozdělila útoky na přijatelné a nepřijatelné. Byly identifikovány čtyři útoky s nepřijatelnou mírou rizika. Konkrétně se jednalo o útok napadení střelnou zbraní, sebevražedný útok s použitím výbušniny, výbušnina v zaparkovaném vozidle a útok s použitím výbušniny bez přítomnosti útočníka. Na každý jeden nadlimitní útok bylo stanoveno okamžité opatření, kořenová příčina a trvalé opatření s následným přepočítáním míry rizika po aplikaci trvalého opatření.

## 6 ETA ANALÝZA

Analýza stromu událostí je aplikovaná na čtyři nejrizikovější hrozby, vyhodnocené pomocí metody FMEA. Jednotlivé scénáře metody ETA analyzují současný stav a stav po aplikaci jednotlivých nápravných opatření. Konkrétně se jedná o čtyři nejrizikovější scénáře:

1. Útok s použitím výbušniny (bez přítomnosti útočnicka).
2. Výbušnina v zaparkovaném vozidle.
3. Sebevražedný útok s použitím výbušniny.
4. Napadení střelnou zbraní.

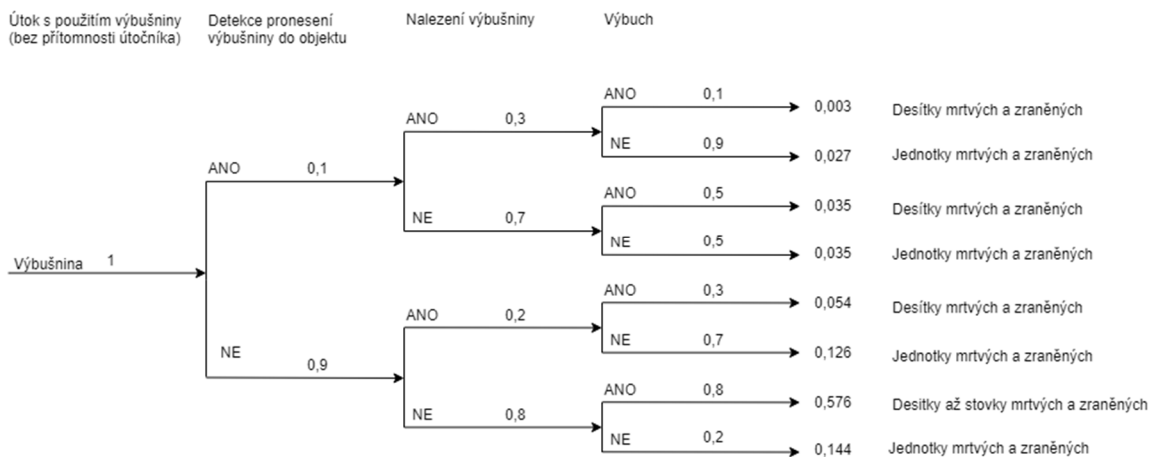
Jednotlivé výstupy scénáře s nápravnými opatřeními a jejich účinností jsou zaznamenány a k nahlédnutí v příloze 1, na konci této práce.

1. Útok s použitím výbušniny (bez přítomnosti útočnicka)

V současné době neexistují žádná opatření, proti možnosti vniknutí osoby do objektu za účelem umístění nebezpečného předmětu ve veřejných prostorech. Pachatel může proniknout do budovy několika způsoby, nejnáze přes hlavní vstup.

Případ, že útočnick pronese výbušninu například v tašce, či jiném zavazadle, které poté opustí v prostorách referenčního objektu, je dle FMEA analýzy nejrizikovějším. Vstup jednotlivých osob do budovy není pod kontrolou a v rámci bezpečnosti neprobíhají ani náhodné kontroly ostrahou či jiné formy bezpečnostních opatření. Proto scénář pronesení časované bomby v zavazadle má vysokou míru rizika.

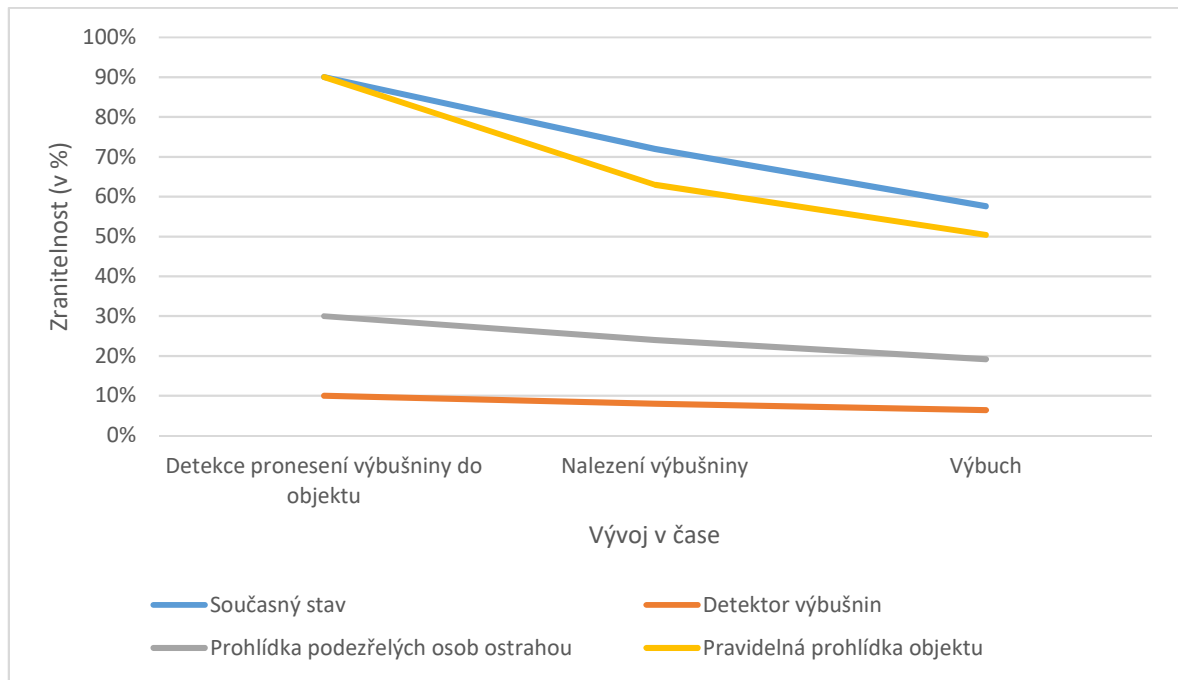
Na níže přiloženém diagramu (Obr. 21) stromu událostí, můžeme vidět současný průběh scénáře útoku s použitím výbušniny bez přítomnosti útočnicka, kde již v základním větvení vidíme vysoký nárůst rizika v důsledku málo pravděpodobné detekce útočnicka s taškou před pronesením výbušniny do objektu. V dalším větvení vidíme i velmi malou pravděpodobnost nalezení výbušniny pracovníkem ostrahy v objektu.



Obrázek 21: Strom událostí před zavedením opatření – útok s použitím výbušniny (bez přítomnosti útočnicka) [zdroj: vlastní]

V návaznosti na současný stav byla vyhodnocena tři nápravná opatření pro potlačení negativního dopadu potenciačního útoku a zvýšení prevence objektu. První opatření navrhuje pravidelné obchůzky objektu ostrahou. Ostraha má k dispozici kamerový systém, sloužící pro kontrolu prostor, avšak v objektu, jakým je FAI, se vyskytuje nemálo míst, které pod dohled kamer nespádají. Nemluvě o ukrytí výbušniny v odpadkovém koši a jiných, kamerou neodhalitelných míst.

Druhým nápravným opatřením je prohlídka podezřelých ostrahou. Opatření obsahuje také namátkové kontroly zavazadel osobám, vstupujícím do objektu a pojí se s ním speciální školení ostrahy. V pořadí třetím nápravným opatřením, a tedy i nejefektivnějším je instalace detektoru výbušnin při vstupu do objektu, kdy by odhalení případné výbušniny bylo okamžité a ostraha by mohla zasáhnout téměř okamžitě. Účinnost všech tří nápravných opatření je promítnuto v grafu (Obr. 22), kde je křivkou zachycen pokles zranitelnosti po uplatnění jednotlivých opatření.

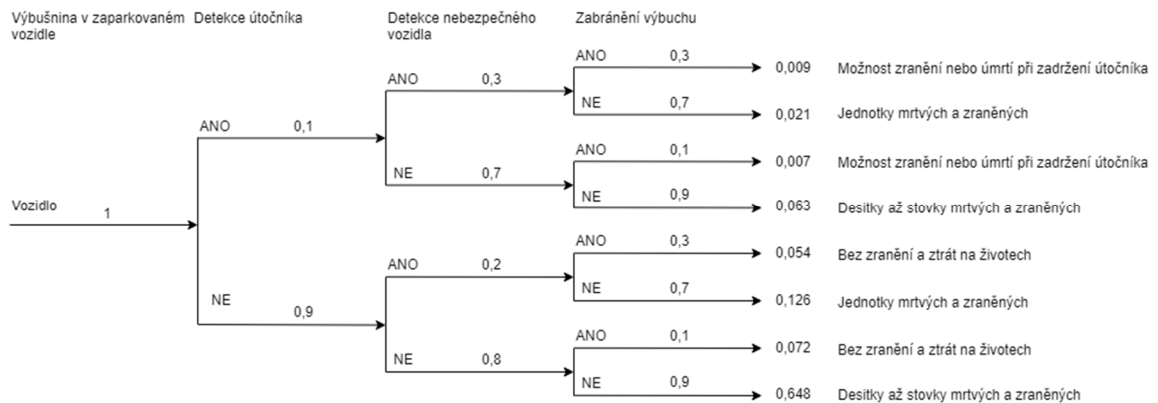


Obr. 22: Graf zachycující vliv nápravných opatření na současný stav (útok s použitím výbuštiny) [zdroj: vlastní]

## 2. Výbušnina v zaparkovaném vozidle

Vzhledem k dislokaci a konstrukci budovy je samotný nájezd automobilem do budovy ne zcela pravděpodobným, oproti tomu zaparkované vozidlo, v němž je umístěna výbušnina, byla odbornou analýzou FMEA zhodnocena jako druhá nejrizikovější. V současné době lze automobil zaparkovat v blízkém okolí budovy ze severní a západní strany referenčního objektu a součást parkoviště se také chodník, který vede k fakultě. Znamená to, že každá osoba, přicházející do objektu fakulty, musí bez výjimky projít určitou částí parkoviště.

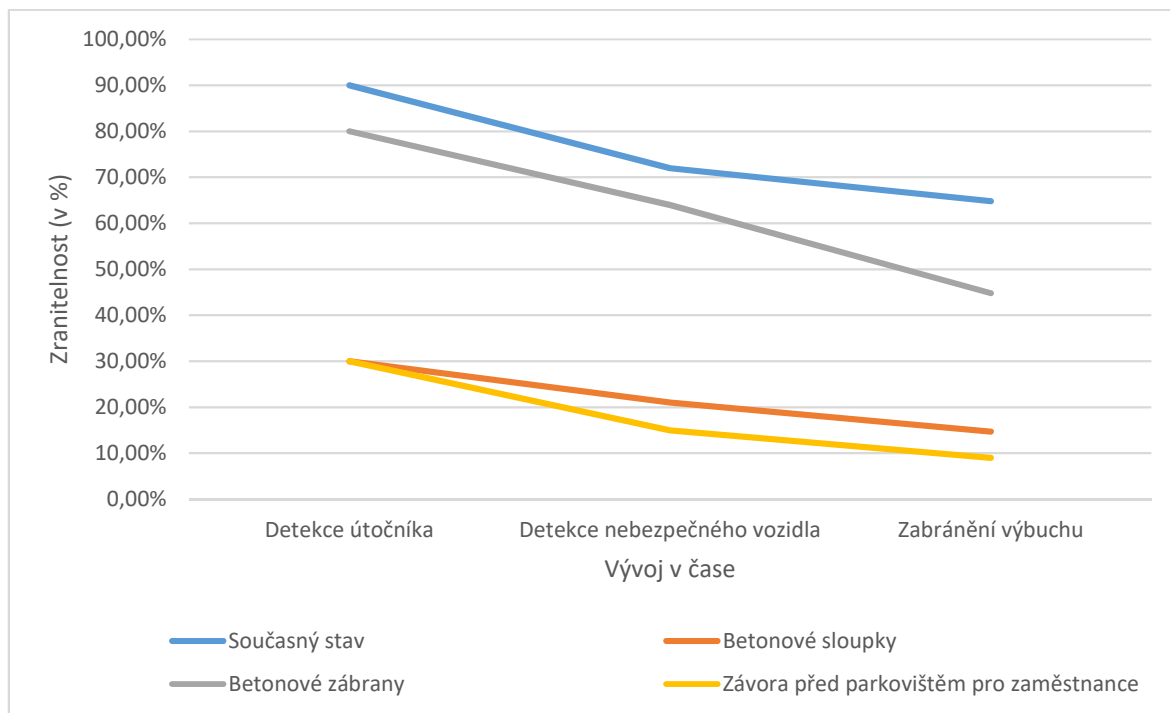
Zároveň se v tomto blízkém okolí pohybují osoby z bytových domů, které zde také parkují svá auta, tudíž detekce případného útočníka je velmi malá, stejně tak, jako detekce podezřelého automobilu s umístěnou bombou. Současný stav je vyobrazen na obrázku (Obr. 23), na jenž navazují tři nápravná opatření pro zmírnění dopadu.



Obr. 23: Strom událostí před zavedením opatření – výbušnina v zaparkovaném vozidle [zdroj: vlastní]

Prvním nápravným opatřením jsou betonové zábrany, které moly splnit účet psychologického charakteru tím, že by mohly potencionálního útočnicka před útokem zneklidnit. Dalším nápravným opatřením jsou zajíždějící betonové sloupky, které by byly součástí každého parkovacího místa v blízkém okolí fakulty a bylo by tak znemožněno stání neznámého majitele aut s tím, že pokud by útočnick automobil nechal mimo parkovací místo, byla by pravděpodobnější detekce.

Třetím a nejefektivnějším nápravným opatřením je závora před parkovištěm pro zaměstnance, která by zcela oddělila prostor pro veřejnost od prostoru fakulty s tím, že by brána měla systém kontroly vstupu s přístupovými úrovněmi pro akademické pracovníky a studenty. Graf obrázku (Obr. 24) znázorňuje snížení míry zranitelnosti objektu po aplikování jednotlivých nápravných opatření.

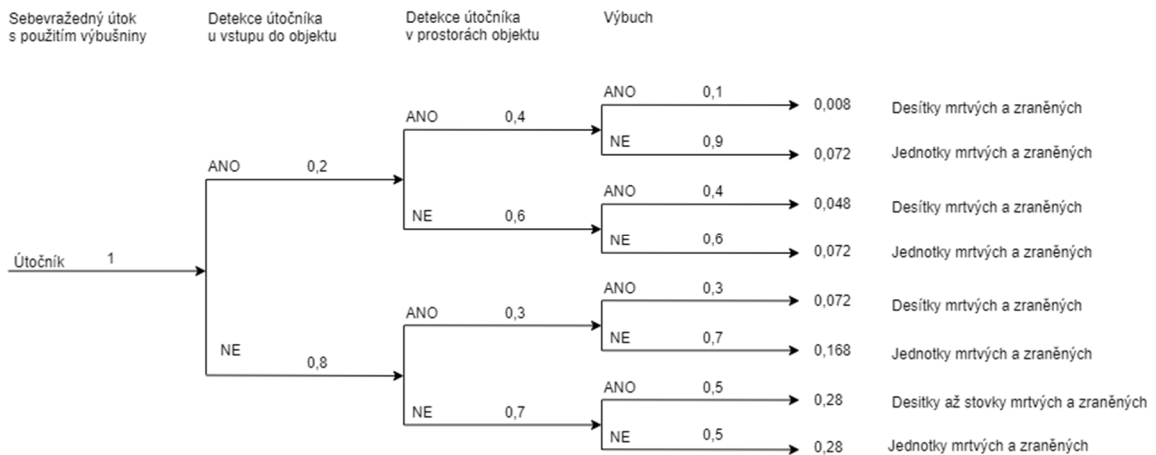


Obr. 24: Graf zachycující vliv nápravných opatření na současný stav (výbušnina v zaparkovaném vozidle) [zdroj: vlastní]

### 3. Sebevražedný útok s výbušninou

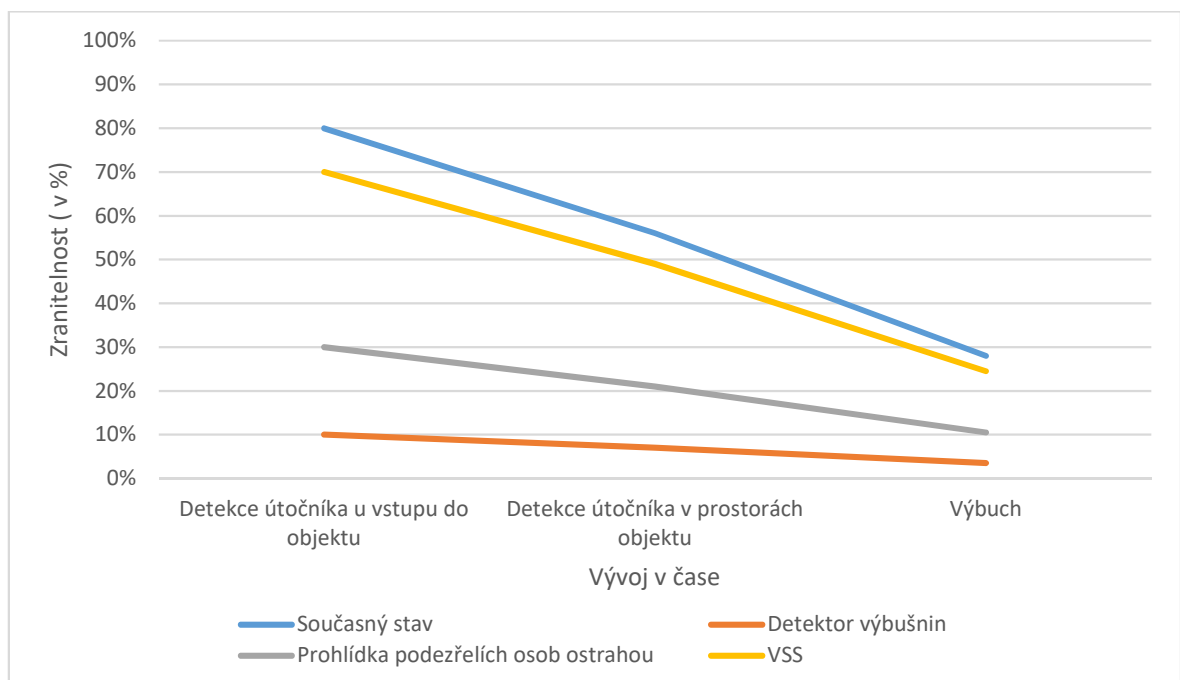
Stejně jako tomu bylo v případě útoku s použitím výbušniny bez přítomnosti útočnicka, jádro bezpečnostního problému vzniká při vstupu do objektu. V analýze se počítá s tím, že výbušnina, umístěna na útočnickovi, je jistou mírou na útočnickovi detekovatelná. Tudíž pravděpodobnost odhalení u vstupu je mírně vyšší, než je tomu u útočnicka s výbušninou v zavazadle. Nicméně právě detekce útočnicka u vstupu, zůstává klíčovou. Současný stav je zachycen na stromu událostí (Obr. 25).





Obr. 25: Strom událostí před zavedením opatření – sebevražedný útok s výbušninou [zdroj: vlastní]

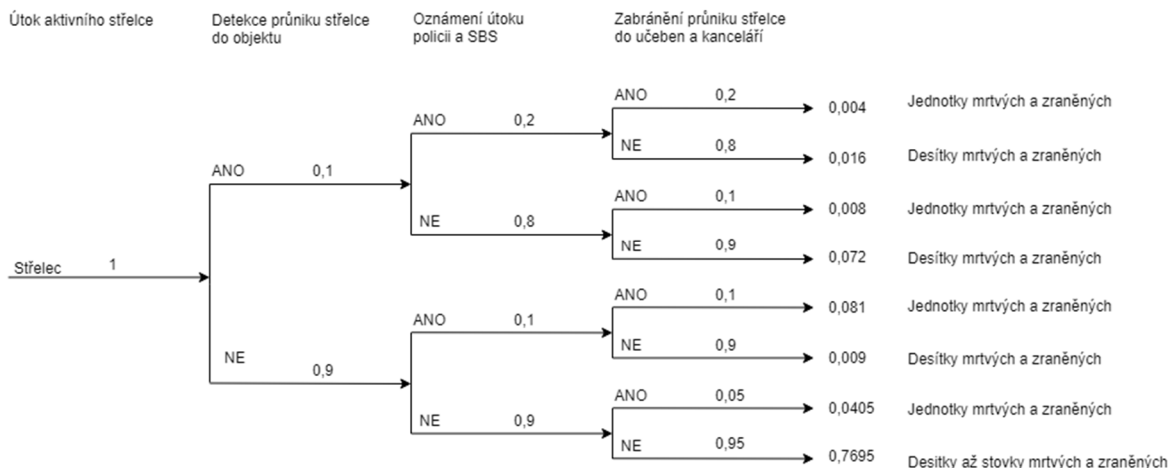
První nápravné opatření (instalování Video Surveillance System) je myšleno z hlediska většího množství umístění kamer se záznamem a osob, dohlížející na kamerový systém v reálném čase, jejichž náplní je pouze a jedině kontrola kamerových záznamů a nikoli další dílčí práce. Druhým nápravným opatřením jsou prohlídky podezřelých osob, s čímž se váže také důkladné odborné školení ostrahy, jak podezřelou osobu vytipovat. Jako nejefektivnějším v tomto případě útoku se jeví detektor výbušnin při vstupu do objektu. Nápravná opatření a jejich účinek na zranitelnost je zachycen obrázkem (Obr. 26).



Obr. 26: Graf zachycující vliv nápravných opatření na současný stav (sebevražedný útok s výbušninou) [zdroj: vlastní]

4. Napadení střelnou zbraní

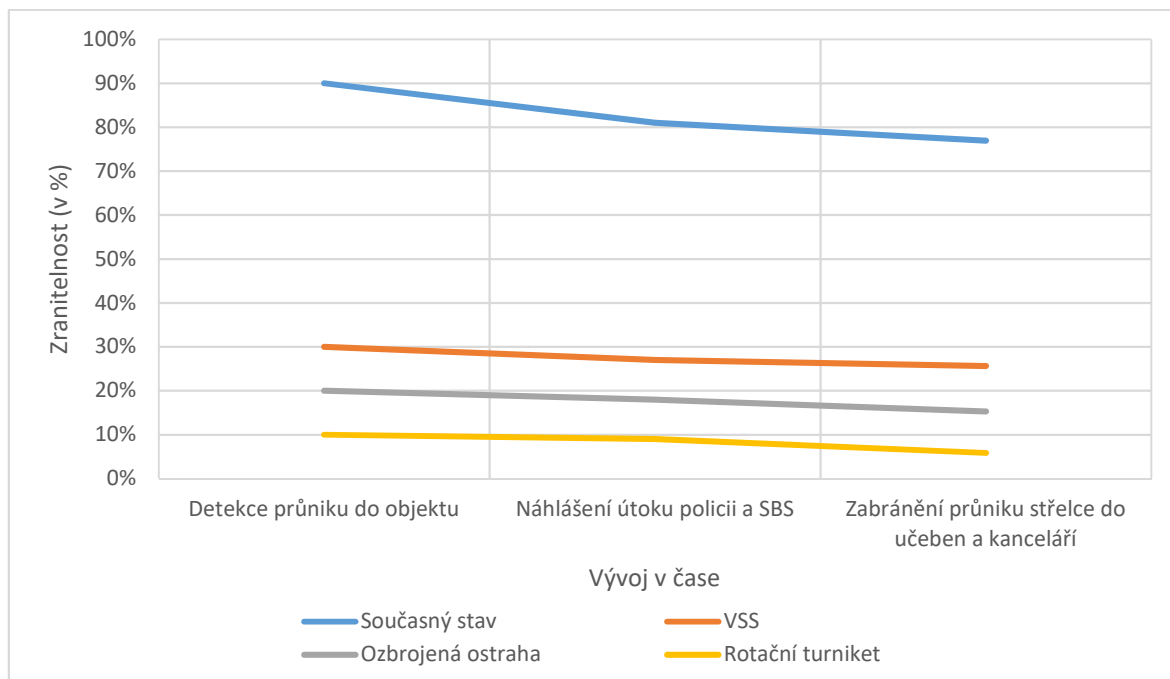
Jako tomu bylo u dvou předchozích útoků (sebevražedný útok s použitím výbušniny a útok pomocí výbušniny bez přítomnosti útočníka) i u útoku střelnou zbraní je zásadní problém v ochraně vstupu do objektu, což současný stav na obrázku (Obr. 27) jasně dokazuje. Obzvláště problematickou částí je samotné detekování útočníka, kdy ukrytí zbraně pod oblečením, je velmi těžce odhalitelné pouhým okem.



Obr. 27: Strom událostí před zavedením opatření – napadení střelnou zbraní [zdroj: vlastní]

Prvním nápravným opatřením v reakci na současný stav referenčního objektu, je větší množství umístěných kamer spolu s osobami, mající v hlavní náplni práce pouze sledování kamerových záznamů pro potřebnou pohotovost v případě útoku.

Druhým opatřením je ozbrojená ostraha, která by mohla v případě nutnosti zasáhnout proti útočníkovi. Jako nejefektivnější navrhaným opatřením jsou rotační turnikety při vstupních dveřích se systémem kontroly vstupu (RFID technologie) a nastavenými přístupovými úrovněmi v návaznosti na status v rámci fakulty.



Obr. 28: Graf zachycující vliv nápravných opatření na současný stav (napadení střelnou zbraní) [zdroj: vlastní]

### Dílčí závěr

Analýza stromu událostí byla aplikována na nadlimitní výsledky analýzy FMEA. Konkrétně se jednalo o útok s použitím výbušniny bez přítomnosti útočníka, výbušninu v zaparkovaném vozidle, sebevražedný útok s použitím výbušniny a napadení střelnou zbraní.

V rámci každého útoku byl stromem událostí (ETA analýza) zhodnocen současný stav referenčního objektu, potažmo forma prevence fakulty vůči konkrétním útokům. Na každý jeden typ útoku byla zpracována tři nápravná opatření, jejichž efektivita byla promítnuta grafem, vystihujícím efektivnost konkrétního opatření ve vztahu s ostatními opatřeními.

## 7 METODA ANALÝZY RIZIK A HROZEB MĚKKÝCH CÍLŮ

V rámci metody Analýzy rizik a hrozeb měkkých cílů je potřeba stanovit umístění útoku a jeho načasování. Co se týče lokace útoku, bere se v potaz útok v objektu a před objektem (myšleno v těsné blízkosti referenčního objektu). V souvislosti s načasováním rozlišujeme dobu mezi 6:00 – 22:00, kdy je objekt otevřen, čas mezi 22:00 – 06:00, kdy je objekt hlídán ostrahou a vstupy do objektu jsou uzamčené a čas v rozmezí 09:00 – 15:00, kdy se v objektu vyskytuje (dle podkapitoly návštěvnosti) nejvíce osob.

Dále je nutno určit pravděpodobnost, že k danému útoku dojde v každé zkoumané variantě (umístění a načasování útoku). Hodnocení probíhá na úrovni dostupnosti, složitosti a atraktivity. Poté se riziko zkoumá z různých podkategorií, specifické pro daný referenční objekt. V případě Fakulty aplikované informatiky se zaměřením na teroristický útok se bude jednat o podkategorie dopadu na životy a na společenství. Každý podkategorie se hodnotí zvlášť, na bodové stupnici od 1 do 7.

- Dostupnost

Na dostupnost je nutno pohlížet z hlediska dostupnosti opatření zbraně, kterou útočník k provedení útoku potřebuje. Jinou dostupnost má například nůž od výbušniny. Také se hodnotí míra nutnosti znalostí k ovládnutí dané útočné zbraně. Míra dostupnosti je vysvětlena a obodována v níže přiložené tabulce (Tab. 17).

Tab. 17: Bodové hodnocení a charakteristika dostupnosti [80]

Bodové hodnocení	Charakteristika
1	Zbraň nebo potřebný materiál k vytvoření zbraně získán kriminální činností, s odbornou praxí anebo dlouhým časem dodání
2	Zbraň nebo potřebný materiál k vytvoření zbraně získán kriminální činností, s odbornou praxí anebo krátkým časem dodání
3	Zbraň nebo potřebný materiál k vytvoření zbraně získán kriminální činností (černý trh apod.) bez potřeby odborných znalostí
4	Zbraň nebo potřebný materiál získán na zvláštní povolení
5	Zbraň nebo vybavení složeno z běžně dostupných prvků
6	Běžně dostupná zbraň či vybavení
7	Beze zbraně

- Složitost

Na složitost je nahlíženo z faktoru ovlivňující náročnost provedení samotného útoku. Zrcadlí v sobě aspekty příprav, provedení a návaznosti útoku. Pokud je za potřebí k jednotlivým fázím pouze jedna osoba anebo si náročnost útoku vyžaduje kooperaci celých skupin. Dále složitost odráží ovlivnitelnost útoku časem a místem, tzn. zdali je útok proveditelný v jakémkoliv čase a lokaci (viz Tab. 18).

Tab. 18: Bodové hodnocení a charakteristika složitosti [80]

Bodové hodnocení	Charakteristika
1	Mezinárodně koordinovaná, dlouhodobě připravovaná akce teroristické skupiny s místem útoku po autorizaci
2	Koordinovaná akce na lokální úrovni se spoluprací s mezinárodní teroristickou skupinou, vstup na autorizaci
3	Jednorázová spolupráce s lokální teroristickou skupinou, místo útoku po autorizaci
4	Dlouhodobá spolupráce s místní kriminální skupinou, nebo autorizace vstupu
5	Jednorázová spolupráce s místní kriminální skupinou, veřejné místo
6	Zapojeno více osob, veřejné místo
7	Bez pomoci, veřejné místo

- Atraktivita

Atraktivitou je myšlena míra atraktivity pro samotné útočníky s aspektem času a místa. Konkrétně se může zahrnovat faktor toho, zda se připravovaný útok již v minulosti v dané lokalitě již stal nebo zda existují informace či obavy, že se k danému útoku schyluje (viz. Tab. 19). Z výše vyjmenovaných podkategorií vyplývá, že při maximálních hodnotách na škále od 1 do 7, může mít maximální součet hodnot 21.

Tab. 19: Bodové hodnocení a charakteristika atraktivity [80]

Bodové hodnocení	Charakteristika
1	Nevyskytuje se u v našem regionu u zvažovaných útočících skupin
2	Výskyt hrozby mimo náš region, avšak zatím bez provedení
3	Hrozba v našem i cizím regionu
4	Realizace mimo náš region bez hrozby v našem regionu
5	Realizace v cizím regionu s hrozbou v našem regionu
6	Ojedinelá realizace v našem regionu
7	Realizace v cizím i našem regionu

- Dopad na životy

Neboli taky dopad na aktivum referenčního objektu odráží, jak velké množství osob by potenciálním útokem bylo zasaženo a jak závažná by byla jejich zranění. Hodnocení probíhá na stupnici od 1 do 7, kde 1 představuje pouze lehký následek ve formě úleku či šoku a na spodní hranici se nachází následek pro osobu nejhorší, čímž je bezprostřední ohrožení života. (viz. Tab. 20) S tím, že výbušninou v seznamu rizik se myslí výbušnina s dopadem na následcích života do 10 m.

Tab. 20: Bodové hodnocení a charakteristika dopadu na životy [80]

Bodové hodnocení	Charakteristika
1	Úlek / šok
2	Lehké zranění bez ohrožení života
3	Vážné zranění s ohrožením života
4	Útok na život jednotlivce
5	Limitovaný dopad na životy osob v bezprostřední blízkosti
6	Bezprostřední ohrožení životů skupiny přítomných
7	Bezprostřední ohrožení životů všech přítomných

- Dopad na společenství

Dopadem na společenství se myslí dopad na komunitu, proti které byl útok vykonán. V případě referenčního objektu této diplomové práce se bude konkrétně jednat o FAI a její zaměstnance, studenty a ostatní osoby spřízněné s tímto objektem.

Maximální součet specifických podkategorií výpočtu analýzy měkkých cílů pro referenční objekt FAI (dopad na společenství a dopad na životy), je 14. Hodnoty dopadu na společenství jsou včetně charakteristiky vystihnuty v tabulce (Tab. 21).

*Tab. 21: Bodové hodnocení a charakteristika dopadu na společenství [80]*

Bodové hodnocení	Charakteristika
1	Bez zjevného dopadu na společenství
2	Slabý dopad na úrovni jednotlivců
3	Lokální omezení aktivit
4	Všeobecná obava jednotlivců
5	Míra ohroženosti při účasti na aktivitách
6	Přerušení činnosti
7	Ukončení účasti nebo činnosti

- Pravděpodobnost hrozby útoku

Příložená tabulka znázorňuje míru hrozby vyjmenovaných jednotlivých násilných útoků na referenční objekt dle specifických faktorů dostupnosti, složitosti a atraktivity. Hodnoty se pohybují mezi mezními hranicemi výše uvedeného výčtu bodového hodnocení konkrétního faktoru.

Tab. 22: Určení dostupnosti, atraktivity a složitosti jednotlivých forem útoku [29, 80]

Útok	Pravděpodobnost (Hrozba)		
	Dostupnost	Atraktivita	Složitost
Napadení chladnou zbraní	6	7	7
Napadení střelnou zbraní	6	7	5
Žhářský útok	6	7	6
Braní rukojmí a barikádová situace	5	5	5
Výbušnina v poštovní zásilce	2	5	5
Sebevražedný útok s použitím výbušniny	2	5	3
Výbušnina v zaparkovaném vozidle	2	5	5
Nájezd vozidla s výbušninou se sebevražedným útočníkem	2	5	3
Útok nájezdem vozidla	5	7	6
Útok s použitím výbušniny (bez přítomnosti útočníka)	2	6	3



- Pravděpodobnost rizika útoku

Tabulka (Tab. 23) popisuje konkrétní rizika výčtu násilných útoků v rámci referenčního objektu. Na rizika se pohlíží z úrovně dopadu na životy, potažmo ohrožení aktiv a dopadu na společenství. Jednotlivé hodnoty jsou v souměřitosti s tabulkami výčtu charakteristik umístěných výše.

Tab. 23: Určení dopadu na životy a na společenství jednotlivých forem útoku [29, 80]

Útok	Pravděpodobnost (Riziko)	
	Dopad na životy	Dopad na společenství
Napadení chladnou zbraní	5	4
Napadení střelnou zbraní	5	5
Žhářský útok	6	6
Braní rukojmí a barikádová situace	2	4
Výbušnina v poštovní zásilce	5	5
Sebevražedný útok s použitím výbušniny	7	6
Výbušnina v zaparkovaném vozidle	4	3
Nájezd vozidla s výbušninou se sebevražedným útočníkem	5	4
Útok nájezdem vozidla	2	3
Útok s použitím výbušniny (bez přítomnosti útočníka)	6	6

- Celkové ohrožení útoku

Tabulka (Tab. 24) znázorňuje úroveň ohrožení, vypočítaného na základě vzorce Ohrožení = Riziko x Hrozba. Ze stanovených hodnot vyplývá, že největší ohrožení je v případě žhářského útoku. Mezní hodnota celkového ohrožení byla dle odborného posouzení stanovena na hodnotu 105 (15 %).

Tab. 24: Výsledná míra ohrožení jednotlivých forem útoku [29, 80]

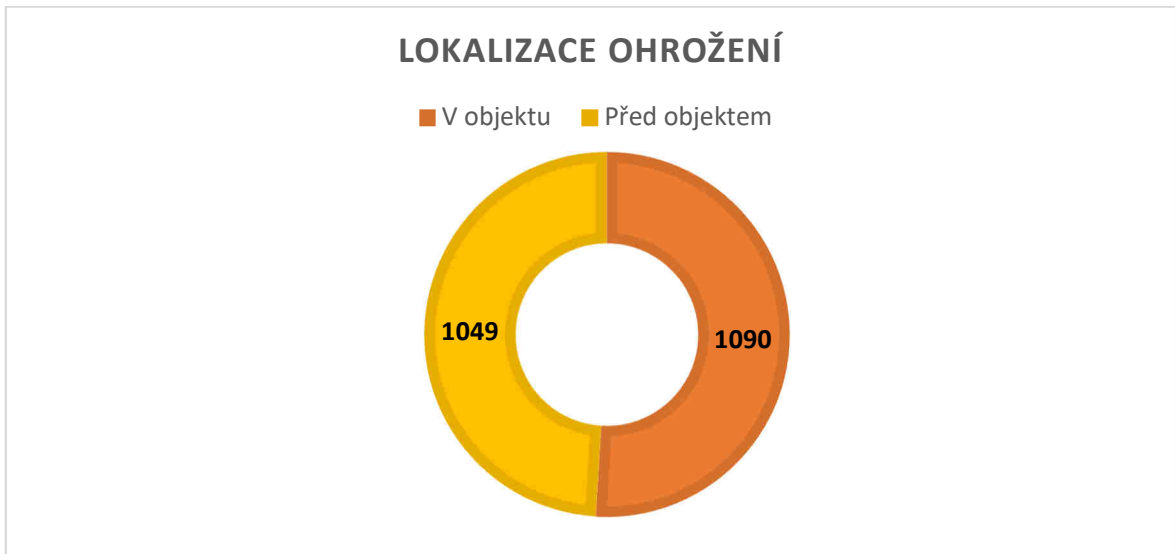
Útok	Hodnocení			
	Součet Hrozeb	Součet Rizik	Celkové Ohrožení	Výsledek
Napadení chladnou zbraní	20	9	180	NOK
Napadení střelnou zbraní	18	10	180	NOK
Žhářský útok	19	12	228	NOK
Braní rukojmí a barikádová situace	15	8	120	NOK
Výbušnina v poštovní zásilce	12	10	120	NOK
Sebevražedný útok s použitím výbušniny	10	13	130	NOK
Výbušnina v zaparkovaném vozidle	12	7	84	OK
Nájezd vozidla s výbušninou se sebevražedným útočником	10	9	90	OK
Útok nájezdem vozidla	18	5	90	OK
Útok s použitím výbušniny (bez přítomnosti útočníka)	11	12	132	NOK

V závislosti na hodnotách překračujících míru přijatelnosti v tabulce (Tab. 24), jsou výsledná rizika podstoupena faktorem místa a doby útoku (viz Tab. 25). K místu útoku „před objektem“ je nutno dodat, že se v těsné blízkosti vstupu před fakultou pravidelně zdržují skupinky akademických pracovníků a studentů, za účelem kouření tabákových výrobků a trávení volného času, a proto na ně byl v rámci analýzy brán zřetel.

Tab. 25: Celková míra ohrožení v závislosti na umístění a načasování útoku [29, 80]

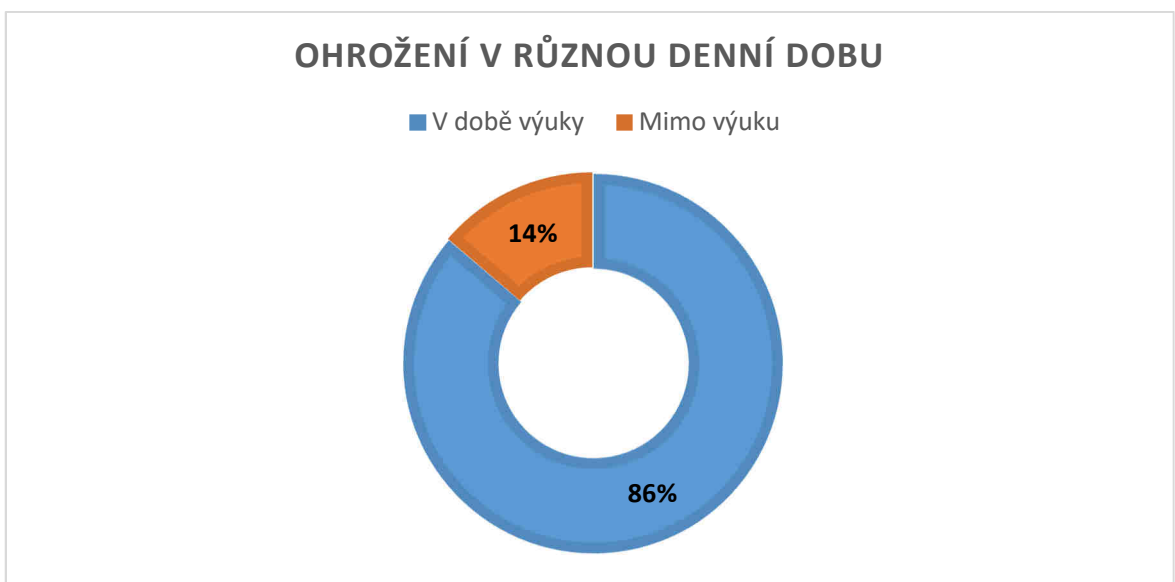
Riziko	Místo útoku	Doba útoku	Hodnocení		
			Součet Hrozba	Součet Riziko	Celkové ohrožení
Napadení chladnou zbraní	v objektu	v době výuky	20	9	<b>180</b>
Napadení chladnou zbraní	před objektem	v době výuky	17	7	<b>119</b>
Napadení chladnou zbraní	před objektem	mimo výuku	x	x	<b>x</b>
Napadení střelnou zbraní	v objektu	v době výuky	18	10	<b>180</b>
Napadení střelnou zbraní	před objektem	v době výuky	16	8	<b>128</b>
Napadení střelnou zbraní	před objektem	mimo výuku	x	x	<b>x</b>
Žhářský útok	v objektu	v době výuky	19	12	<b>228</b>
Žhářský útok	před objektem	v době výuky	17	12	<b>204</b>
Žhářský útok	před objektem	mimo výuku	21	14	<b>294</b>
Braní rukojmí a barikádová situace	v objektu	v době výuky	15	8	<b>120</b>
Braní rukojmí a barikádová situace	před objektem	v době výuky	14	7	<b>98</b>
Braní rukojmí a barikádová situace	před objektem	mimo výuku	x	x	<b>x</b>
Výbušnina v poštovní zásilce	v objektu	v době výuky	12	10	<b>120</b>
Výbušina v poštovní zásilce	před objektem	v době výuky	x	x	<b>x</b>
Výbušina v poštovní zásilce	před objektem	mimo výuku	x	x	<b>x</b>
Sebevražedný útok s použitím výbušniny	v objektu	v době výuky	10	13	<b>130</b>
Sebevražedný útok s použitím výbušniny	před objektem	v době výuky	8	12	<b>96</b>
Sebevražedný útok s použitím výbušniny	před objektem	mimo výuku	x	x	<b>x</b>
Útok s použitím výbušniny (bez přítomnosti útočníka)	v objektu	v době výuky	11	12	<b>132</b>
Útok s použitím výbušniny (bez přítomnosti útočníka)	před objektem	v době výuky	10	11	<b>110</b>
Útok s použitím výbušniny (bez přítomnosti útočníka)	před objektem	mimo výuku	x	x	<b>x</b>

Z výpočtu lze tedy říct (viz. Obr. 29), že lokalizace útoku před objektem nebo v objektu je téměř totožná. Způsobuje to zejména faktor vysoké koncentrace osob před hlavním vstupem do objektu, obzvláště v pravidelných prodlevách mezi výukami, pauzami a volným časem aktiva referenčního objektu.



Obr. 29: Výsledek výpočtu ohrožení v závislosti na lokalizaci útoku [zdroj: vlastní]

Obrázek (Obr. 30) zachycuje výsledek výpočtu ohrožení v závislosti na denní době útoku a vidíme tedy, že ohrožení studentů a akademických pracovníků fakulty je zejména v čase, kdy probíhá výuka.



Obr. 30: Výsledek výpočtu ohrožení v závislosti na denní době útoku [zdroj: vlastní]

- Návrh nápravného opatření

Na základě výsledků analýzy rizik a hrozeb měkkých cílů byla stanovena vhodná nápravná opatření (Tab. 26). Konkrétní návrhy nezohledňují aspekty pořizovacích a provozních nákladů, náročnosti realizace, servisu, údržby apod. U každého návrhu je součástí posílení bezpečnostního kamerového systému. Obzvlášť je zapotřebí dbát důraz na posílení personální stránky, hlavně z hlediska personální stránky, kdy ostraha v rámci své služby bude zodpovědná pouze a jenom za správu kamerového systému a řešení vyskytnutého bezpečnostního problému.

Druhým z nejčastějších prvků objevující se v tabulce nápravných opatření, je rotační turniket s RFID technologií, který by také pomohl k evidenci počtu osob, vyskytujících se v referenčním objektu, což by pomohlo například v případě nutné okamžité evakuace.

Tab. 26: Návrh nápravných opatření teroristických útoků [zdroj: vlastní]

Typ útoku						
Napadení chladnou zbraní	Napadení střelnou zbraní	Sebevražedný útok s použitím výbušniny	Útok s použitím výbušniny bez přítomnosti útočnicka	Žhářský útok	Braní rukojmí a barikádová situace	Výbušnina v poštovní zásilce
Návrh nápravného opatření - venkovní						
VSS	VSS	VSS	VSS	Osvětlení na fotočidlo a VSS	VSS	VSS
Návrh nápravného opatření - vnitřní						
Rotační turniket s RFID technologií a detektor kovů	Rotační turniket s RFID technologií	Detektor výbušnin	Detektor výbušnin	Vnitřní rozhlas	Rotační turniket s RFID technologií	Detektor výbušnin

### Dílčí závěr

Metoda analýzy rizik a hrozeb měkkých cílů pojednávala o útocích z úhlu pohledu dostupnosti, složitosti, atraktivity a následném dopadu na společenství a na životy. Po určení pravděpodobnosti rizika a hrozby se jejich násobkem stanovila míra celkového ohrožení, které rozdělilo útoky na přijatelné a nepřijatelné. Návazně na to byla nepřijatelná rizika ohodnocena z aspektu místa a doby provedení útoku. Z výsledku celkového ohrožení podléhajícímu faktoru času a lokalizace, vzešla stanoviska, že referenční objekt je v největším ohrožení v době výuky na fakultě. Na základě těchto zjištění byla vybrána vhodná vnitřní a venkovní bezpečnostní opatření.

## ZÁVĚR

Cílem této diplomové práce bylo provedení analýzy rizik s následným navrhnutím vhodných bezpečnostních opatření pro daný referenční objekt. Teoretická část se v úvodu zabývala tematikou terorismu, vymezením jeho pojmu a zmapováním této problematiky ve světě a na území České republiky. Vývoj terorismu byl rozčleněn do jednotlivých etap a byly popsány charakteristické prvky jednotlivých období, spolu se stručným představením nejznámějších teroristických organizací.

Dále bylo na terorismus pohlíženo ze strany měkkých cílů aneb jejich míra ohrožení teroristickými útoky. Pro stanovení míry rizika bylo zapotřebí jejich analyzování, proto se následující část věnovala charakteristice a konkrétním typům metodik, vhodných pro výpočet bezpečnostní analýzy rizik.

V úvodu praktické části došlo k prezentaci fakulty. Konkrétně bylo popsáno prostředí, ve kterém se fakulta nachází včetně budov v její těsné blízkosti. Poté byla popsána budova fakulty jako taková, byly specifikovány její procesy, návštěvnost a identifikována aktiva referenčního objektu. Na základě charakteristiky stanovené v teoretické části, byly vybrány tři metodiky analýzy rizik, na jejichž výsledcích byla navrhována vhodná nápravná bezpečnostní opatření. Práce tak zrcadlí současnou bezpečnostní situaci fakulty a pojednává o možných vylepšeních.

Věřím, že výstupy této diplomové práce budou inspirací pro klíčové osoby referenčního objektu a budou se podílet na pozitivní změně bezpečnostní situace.

## SEZNAM POUŽITÉ LITERATURY

- [1] SCHMID, Alex Peter a A. J JONGMAN. *Political terrorism: a new guide to actors, authors, concepts, data bases, theories, & literature*. Rev., expanded, and updated ed. New Brunswick, N.J.: Transaction Publishers, [2005]. ISBN 9781412804691.
- [2] SMOLÍK, Josef. *Úvod do studia mezinárodních vztahů*. Praha: Grada, 2014. ISBN 9788024751313.
- [3] MAREŠ, Miroslav. *Terorismus v ČR*. Brno: Centrum strategických studií, 2005. ISBN 9788090333383.
- [4] *Latdict* [online]. Washington: Kevin Mahoney, 2006 [cit. 2019-04-04]. Dostupné z: [www.latin-dictionary.net](http://www.latin-dictionary.net)
- [5] *11. září 2001*. Deset let poté. Praha: Cepin, 2011. ISBN 978-80-87460-06-1.
- [6] ZEMAN, Jan. *Terorismus: historicko-psychologická studie*. Praha: Triton, 2002. ISBN 80-725-4305-9.
- [7] FILIPEC, Ondřej. *Fenomén terorismus: česká perspektiva*. 1. Olomouc: UPOL, 2017. ISBN 978-80-244-5040-7.
- [8] *WULFLUND: We make history come alive!* [online]. London: wulflund, 2019 [cit. 2019-04-04]. Dostupné z: [www.wulflund.com](http://www.wulflund.com)
- [9] TELIČKA, Marek. Velé objevy: 5 geniálních vynálezů staré Číny. *100 + 1: zahraniční zajímavosti* [online]. Brno: Extra Publishing, 2014, 22. 12. 2014 [cit. 2019-04-27]. Dostupné z: <https://www.stoplusjednicka.cz/velke-objevy-5genialnich-vynalezu-stare-ciny>
- [10] *Terrorism and Literature: Edited by Peter C. Herman*. 1. London: Cambridge University Press, 2018. ISBN 9781316987292.
- [11] Secretary, People's Union for Democratic Rights. *Death Penalty, TADA, and the Rajiv Gandhi Assassination Case*. 1. Delhi: Secretary, People's Union for Democratic Rights, Delhi, 1998. ISBN 2112917.
- [12] 60 killed by Beirut car bomb: US carrier heads for Lebanon in readiness for evacuation. *The Guardian: Available for everyone, funded by readers* [online]. London: The Guardian [cit. 2019-04-04]. Dostupné z: <https://www.theguardian.com/theguardian/1985/mar/09/fromthearchive>
- [13] LATSON, Jennifer. How a Religious Sect Rooted in Yoga Became a Terrorist Group. *Www.time.com* [online]. New York: Time, 1995, 20. 03. 2015 [cit. 2019-04-04]. Dostupné z: [time.com/3742241/tokyo-subway-attack-1995/](http://time.com/3742241/tokyo-subway-attack-1995/)
- [14] CHARVÁT, Jan. *Současný politický extremismus a radikalismus*. Praha: Portál, 2007. ISBN 9788073670986.



- [15] LUKÁŠEK, Libor. *Fenomén mezinárodního terorismu ve světle současného mezinárodního práva*. Plzeň: Západočeská univerzita, 1999. ISBN 80-7082-571-5.
- [16] VON MISES, Ludwig. *Lidské jednání: pojednání o ekonomii*. Přeložil Josef ŠÍMA. Praha: Liberální institut, 2006. ISBN 8086389456.
- [17] SMITH, G. Davidson. *Combating Terrorism*. 1. Michigan: University of Michigan Press, 1990. ISBN 978-0415030670.
- [18] VISINGR, Lukáš. TOP 10 zbraní amerických speciálních jednotek: 1. část. *Radio Dixie: Sounds of America* [online]. Pardubice: Radiodixie.cz, 2019, 02. 06. 2017 [cit. 2019-04-04]. Dostupné z: <http://www.radiodixie.cz/clanek/top-10-zbrani-americkych-specialnich-jednotek-1-cast>
- [19] HRAZDÍRA, Ivo, Libor KOVÁRNÍK a František NOVOTNÝ. *Použití zbraně a zákon*. 1. Praha 8: EUROUNION, s. r. o, 2000. ISBN 80-858558-83-5.
- [20] Typologie terorismu. *Ministerstvo vnitra České republiky* [online]. Praha: Odbor bezpečnostní politiky, 2009, 09. 06. 2009 [cit. 2019-04-04]. Dostupné z: <https://www.mvcr.cz/clanek/typologie-terorismu.aspx?q=Y2hudW09Mw%3D%3D>
- [21] TUREČEK, Jaroslav. *Policejní pyrotechnika*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2014, 282 s. ISBN 978-80-7380-510-4.
- [22] FILIPEC, Ondřej. *Úvod do problematiky zbraní hromadného ničení*. Olomouc, 2013. ISBN 978-80-244-3810-8.
- [23] JANOŠEC, Josef. *O terorismu: pro pracovníky bezpečnostního systému*. V Ostravě: Sdružení požárního a bezpečnostního inženýrství, 2010, 108 s. SPBI Spektrum. Červená řada. ISBN 978-80-7385-097-5.
- [24] BRZYBOHATÝ, Marian. *Terorismus I*. 1. Praha: Ministerstvo obrany České republiky, 1999. ISBN 80-902670-1-7.
- [25] *Global Terrorism Database* [online]. United States: University of Maryland, 2018 [cit. 2019-04-04]. Dostupné z: <http://www.start.umd.edu/>
- [26] *Europol* [online]. The Netherlands: A body of the European Union, 2018 [cit. 2019-04-04]. Dostupné z: [www.europol.europa.eu](http://www.europol.europa.eu)
- [27] EU terrorism situation and trend report: Reviewing the terrorism phenomenon. *Europol* [online]. The Netherlands: A body of the European Union, 2019, 2017 [cit. 2019-04-04]. Dostupné z: <https://europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report>
- [28] EU terrorism situation and trend report: Reviewing the terrorism phenomenon. *Europol* [online]. The Netherlands: A body of the European Union, 2018, 20.06.2018 [cit. 2019-04-04]. Dostupné z: <https://europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report#fndtn-tabs-0-bottom-2>
- [29] KALVACH, Zdeněk. *Základy ochrany měkkých cílů metodika*. Praha: Ministerstvo vnitra České republiky, 2016.

- [30] Analýzy: Přehled teroristických útoků za rok 2018. *Ministerstvo vnitra České republiky: Centrum proti terorismu a hybridním hrozbám* [online]. Praha: MVČR, 2019 [cit. 2019-05-01]. Dostupné z: <https://www.mvcr.cz/cthh/clanek/prehled-teroristickych-utoku-za-rok-2018.aspx>
- [31] World Facts: Worst Terrorist Attacks In World History. *Worldatlas: Witness Our Great Big World*. [online]. Quebec: Marek Brys, 1994, 19. 03. 2019 [cit. 2019-04-04]. Dostupné z: <https://www.worldatlas.com/articles/worst-terrorist-attacks-in-history.html>
- [32] Religious demography: Czech republic. *Global Religious Futures: Pew-Templeton Project* [online]. Washington, 1990, 2017 [cit. 2019-04-04]. Dostupné z: [http://www.globalreligiousfutures.org/countries/czech-republic#/?affiliations\\_religion\\_id=0&affiliations\\_year=2010&ion\\_name=All%20Countries&restrictions\\_year=2016](http://www.globalreligiousfutures.org/countries/czech-republic#/?affiliations_religion_id=0&affiliations_year=2010&ion_name=All%20Countries&restrictions_year=2016)
- [33] ŠIMÁNEK, Vít. Senior se přiznal k útokům na trať, chtěl varovat před migranty. *České noviny* [online]. Praha: ČTK, 2019, 07. 01. 2019 [cit. 2019-04-04]. Dostupné z: <https://www.ceskenoviny.cz/zpravy/soud-s-obzalovanym-z-terorismu-kvuli-srazkam-vlaku-se-stromy/1706216>
- [34] EICHLER, Jan. *Bezpečnostní a strategická kultura mezinárodních organizací a ČLR*. 1. Praha: Oeconomica, 2013. ISBN 978-80-245-1991-0.
- [35] SAIKIA, Jaideep a E. A. STEPANOVA. *Terrorism: patterns of internationalization*. Thousand Oaks, Calif.: SAGE, 2009. ISBN 978-81-7829-951-8.
- [36] EICHLER, Jan. *Terorismus a války na počátku 21. století*. 1. Praha 1: Karolinum, 2007. ISBN 978-80-246-1317-8.
- [37] BRZYBOHATÝ, Marian. *Terorismus*. Praha: Police History, 1999. ISBN 80-902670-4-1.
- [38] *Terorismus a my: základy sebeobrany*. Praha 4: Computer Press, 2001. ISBN 80-7226-584-9.
- [39] INTROVIGNE, Massimo. *Hamás: islámský terorismus ve Svaté zemi*. Praha: Vyšehrad, 2003. Moderní dějiny (Vyšehrad). ISBN 80-702-1659-x.
- [40] ARTHUR, Paul a Kimberly COWELL-MEYERS. Irish Republican Army: Irish military organization. *Encyclopedia Britannica* [online]. 2018, 2018 [cit. 2019-05-01]. Dostupné z: <https://www.britannica.com/topic/Irish-Republican-Army>
- [41] HAYS, Jeffrey. TRIADS AND ORGANIZED CRIME IN CHINA. *Fact and details* [online]. 2008, 2012 [cit. 2019-01-21]. Dostupné z: <http://factsanddetails.com/china/cat8/sub50/item300.html>
- [42] MOGHADAM, Assaf. *The globalization of martyrdom: Al Qaeda, Salafi Jihad, and the diffusion of suicide attacks*. Baltimore: Johns Hopkins University Press, 2008. ISBN 978-0-8018-9055-0.

- [43] MAKARIUSOVÁ, Radana. *Terorismus, globální terorismus a éra al-Káidy*. Praha: Metropolitan University Prague Press, 2013. ISBN 978-80-86855-95-0.
- [44] WEISS, Michael a Hassan HASSAN. *Islámský stát: uvnitř armády teroru*. Brno: CPress, 2015, 255 s. ISBN 978-80-264-0883-3.
- [45] BBC: News Magazine. *BBC* [online]. London: BBC, 2019, 2014 [cit. 2019-05-05]. Dostupné z: <https://www.bbc.com/news/blogs-magazine-monitor-27390954>
- [46] CURRIE, Stephen. *Terrorists and terrorist groups*. San Diego, Calif.: Lucent Books, c2002. ISBN 9781590182079.
- [47] Bezpečnostní politika: Ochrana měkkých cílů. *Ministerstvo vnitra České republiky* [online]. Praha: MVČR, 2019 [cit. 2019-05-01]. Dostupné z: <https://www.mvcr.cz/clanek/ochrana-mekkych-cilu.aspx>
- [48] HESTERMAN, Jennifer L. *Soft target hardening: protecting people from attack*. Boca Raton: CRC Press, Taylor & Francis Group, [2015], xxii, 299 s. ISBN 978-1-4822-4421-2.
- [49] ČR. *STRATEGIE ČESKÉ REPUBLIKY PRO BOJ PROTI TERORISMU: Opatření, zaměřená na minimalizaci rizik a dopadů potenciálních teroristických ptoků na území České republiky a proti zájmům České republiky v zahraničí*. In: Praha: Ministerstvo vnitra České republiky, 2013, ročník 2013, číslo 1.
- [50] ŠEFČÍK, Vladimír. *Analýza rizik*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009, 98, s. ISBN 978-80-7318-696-8.
- [51] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada). ISBN 978-802-4730-51-6.
- [52] ANTUŠÁK, Emil. *Krizový management: hrozby - krize - příležitosti*. Praha: Wolters Kluwer Česká republika, 2009. ISBN 978-807-3574-888.
- [53] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management*. Zlín: Radim Bačuvčík - VeRBuM, 2015. ISBN 978-80-87500-19-4.
- [54] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management*. Zlín: Radim Bačuvčík - VeRBuM, 2015. ISBN 978-80-87500-35-4.
- [55] Masakr v Česku: Tragédii v Uherském Brodě sledují ve světových médiích. *Lidovky* [online]. Praha: Lidovky, 2015, 2019 [cit. 2019-05-01]. Dostupné z: [www.lidovky.cz](http://www.lidovky.cz)
- [56] Terrorist drives truck through a Bastille Day celebration. *HISTORY* [online]. London: A&E Television Networks, 2019, March 7, 2019 [cit. 2019-05-01]. Dostupné z: <https://www.history.com/this-day-in-history/2016-nice-terrorist-attacks>
- [57] How Berlin is marking the 2nd anniversary of the Christmas market terror attack. *The Local: de* [online]. Stockholm, 2019, 2018 [cit. 2019-05-01]. Dostupné z: <https://www.thelocal.de/20181219/how-berlin-is-commemorating-victims-of-the-christmas-market-attack-on-second-anniversary>

- [58] TVRDEK, Jan a Ondrej TARČÁNI. *Měkké cíle: aktuální problematika v boji proti terorismu*. V. Praha: Ochrana a Bezpečnost, 2016. ISSN 1805 - 5656.
- [59] PAVLÍČEK, Luboš. Mladá žena zavraždila studenta – chránil spolužačku. *Česká televize* [online]. Praha, 2019, 14. 10. 2014 [cit. 2019-05-06]. Dostupné z: <https://ct24.ceskatelevize.cz/domaci/1013782-mlada-zena-zavrazdila-studenta-chranil-spoluzacku>
- [60] BUZALKA, Ján. *Teória bezpečnostných rizík*. Bratislava: Akadémia Policajného zboru, 2012, 167 s. ISBN 978-80-8054-547-5.
- [61] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 2., aktualiz. a rozš. vyd. Praha: Grada, c2006, 296 s. Expert. ISBN 80-247-1667-4.
- [62] WHEELER, Evan. *Security risk management: building an information security risk management program from the ground up*. Waltham, MA: Syngress, 2011, 1 online zdroj (xxi, 340 s.). ISBN 978-1-59749-615-5.
- [63] REITŠPÍŠ, Josef. *Manažerstvo bezpečnostných rizík*. Žilina: Žilinská univerzita v Žiline, 2004. Vysokoškolské učebnice. ISBN 80-8070-328-0.
- [64] DRENNAN, Lynn T. a Allan MCCONNELL. *Risk and crisis management in the public sector*. New York: Routledge, 2007. Routledge masters in public management series. ISBN 978-0415378147.
- [65] ČR. *Seznam - Přehled metodik pro analýzu rizik: GRHZS*. In: . Brno: Ministerstvo vnitra, Generální ředitelství HZS ČR, 2004, ročník 1, číslo 1. Dostupné také z: <http://krizport.firebrno.cz/dokumenty/seznam-prehled-metodik-pro-analyzu-rizik>
- [66] LÁTAL, I., ŠTAJNERSKÝ, M.: *Bezpečnostní zásady ochrany podniku: prevence a řešení krizových situací*, 4. vydání, Praha: PROSPEKTUM, 2001, 120 str., ISBN 80-7175-091-3.
- [67] KYNCL, Jaromír. *Bezpečnost objektu ve světle moderních technologií*. Praha: Komora podniků komerční bezpečnosti České republiky, 2014. ISBN 978-80-260-7115-0.
- [68] ZUZÁK, Roman. *Krizové řízení podniku: dokud ještě není v krizi*. Praha: Professional Publishing, 2004, 179 s. ISBN 8086419746.
- [69] RYDVALOVÁ, Petra a Jiří RYDVAL. *Outsourcing ve firmě: průvodce pro manažera s tipy pro české prostředí*. Brno: Computer Press, 2007, vii, 102 s. ISBN 9788025118078.
- [70] *Univerzita Tomáše Bati ve Zlíně: Fakulta aplikované informatiky* [online]. Zlín: UTB, 2019 [cit. 2019-05-01]. Dostupné z: [www.fai.utb.cz](http://www.fai.utb.cz)
- [71] *Oficiální stránky statutárního města Zlína* [online]. Zlín: Zlín, 2019 [cit. 2019-05-01]. Dostupné z: [www.zlin.eu](http://www.zlin.eu)
- [72] *Bamboo: Caribbean food and cocktail* [online]. Zlín: Zlín, 2019 [cit. 2019-05-05]. Dostupné z: [www.bambooclub.cz](http://www.bambooclub.cz)

- [73] Mapy [online]. Praha: seznam.cz, 2019 [cit. 2019-05-05]. Dostupné z: [www.mapy.cz](http://www.mapy.cz)
- [74] Mapa kriminality [online]. Praha: Projekt Otevřené společnosti, 2019 [cit. 2019-05-01]. Dostupné z: <http://www.mapakriminality.cz>
- [75] Mapy Google [online]. Silicon Valley: Google, 2005 [cit. 2019-05-01]. Dostupné z: [www.google.com/maps/](http://www.google.com/maps/)
- [76] STALMACH, Jan. Faculty of applied informatics in Zlin. In: Jan Stalmach: homepage [online]. Zlín: download.html, 2007, 2007 [cit. 2019-05-07]. Dostupné z: <https://www.stalmach.name/data/utb2007.jpg>
- [77] Interaktivní mapa budovy: U5 [online]. Zlín: UTB, 2019 [cit. 2019-05-05]. Dostupné z: <http://www.imb.fai.utb.cz/>
- [78] Data z informačního systému Fakulty aplikované informatiky. Zlín, 2019.
- [79] Časový plán výuky a akcí spojených s výukou na FAI UTB ve Zlíně pro akademický rok 2019/ 2020. Zlín, 2019. Dostupné také z: <https://fai.utb.cz/o-fakulte/uredni-deska/harmonogram-akademickeho-roku/>
- [80] KALVACH, Zdeněk. Metodika pro analýzu hrozeb a rizik pro měkké cíle. 1. Praha, 2017.

**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK**

EU	Evropská unie.
ČR	Česká republika.
FAI	Fakulta aplikované informatiky.
UTB	Univerzita Tomáše Bati.
MVČR	Ministerstvo vnitra České republiky.
GTD	Global Terrorism Database.
ETA	Euskadi ta Askatasuna.
IRA	Irská republikánská armáda.
ISIS	Islámský stát v Iráku a Sýrii.
CL	Check List.
WI	What If Analysis.
SA	Safety Audit.
PHA	Preliminary Hazard Analysis
HAZOP	Hazard Operation Precess.
ETA	Event Tree Analysis.
FTA	Fault Tree Analysis.
HRA	Human Reliability Analysis.
HTA	Hazard Tree Analysis.
RR	Relative Ranking.
CCA	Causes and Consequences Analysis.
STA	Soft Targets Analysis.
IZS	Integrovaný záchranný systém.
FMEA	Failure Mode and Effect Analysis.
VTP-ICT	Vědeckotechnický park Informační a komunikační technologie.

---

U51	(Západní pavilon A) Nad stráněmi 4511, Zlín.
U52	(Severní pavilon B) Nad stráněmi 4511, Zlín.
U53	(Východní pavilon C) Nad stráněmi 4511, Zlín.
U54	(Jižní pavilon D) Nad stráněmi 4511, Zlín.
U55	(Tělocvična E) Nad stráněmi 4511, Zlín.
VSS	Video Surveillance Systém.
RFID	Radio Frequency Identification.
PZTS	Poplachový zabezpečovací a tísňový systém.
EPS	Elektrická požární signalizace.
CCTV	Closed-circuit television.
PIR	Pasivní infračervené čidlo.

**SEZNAM OBRÁZKŮ**

Obr. 1: Fáze útoku .....	19
Obr. 2: Počet zatčených podezřelých za náboženský terorismus od roku 2012 do 2016 v Evropské Unii .....	20
Obr. 3: Procentuální zastoupení jednotlivých typů teroristických útoků.....	21
Obr. 4: Procentuální vyjádření cílů teroristických útoků.....	30
Obr. 5: Grafické znázornění analýzy rizik.....	36
Obr. 6: Rozdělení metodiky analýzy rizik .....	39
Obr. 7: Umístění budovy U5 ve Zlíně .....	48
Obr. 8: Dislokace FAI, VTP-ICT a Bamboo clubu ve Zlíně.....	50
Obr. 9: Mapa kriminality Zlínského kraje .....	51
Obr. 10: Fakulta aplikované informatiky ve Zlíně .....	53
Obr. 11: První podlaží budovy U5 .....	54
Obr. 12: Druhé podlaží budovy U5 .....	55
Obr. 13: Třetí podlaží budovy U5.....	56
Obr. 14: Čtvrté až osmé podlaží budovy U5 .....	56
Obr. 15: Hlavní procesy objektu.....	57
Obr. 16: Věda a výzkum .....	58
Obr. 17: Výuka .....	59
Obr. 18: Řízení fakulty .....	60
Obr. 19: Ostatní podpůrné činnosti.....	61
Obr. 20: Průměrná přítomnost studentů a učitelů v budově U5 ve všedních dnech letního semestru akademického roku 2018/ 2019 .....	65
Obr. 21: Strom událostí před zavedením opatření – útok s použitím výbušniny (bez přítomnosti útočníka) .....	76
Obr. 22: Graf zachycující vliv nápravných opatření na současný stav (útok s použitím výbušniny) .....	77
Obr. 23: Strom událostí před zavedením opatření – výbušnina v zaparkovaném vozidle .....	78
Obr. 24: Graf zachycující vliv nápravných opatření na současný stav (výbušnina v zaparkovaném vozidle).....	79
Obr. 25: Strom událostí před zavedením opatření – sebevražedný útok s výbušninou .....	80



Obr. 26: Graf zachycující vliv nápravných opatření na současný stav (sebevražedný útok s výbušninou) .....	80
Obr. 27: Strom událostí před zavedením opatření – napadení střelnou zbraní.....	81
Obr. 28: Graf zachycující vliv nápravných opatření na současný stav (napadení střelnou zbraní).....	82
Obr. 29: Výsledek výpočtu ohrožení v závislosti na lokalizaci útoku.....	91
Obr. 30: Výsledek výpočtu ohrožení v závislosti na denní době útoku .....	91

**SEZNAM TABULEK**

Tab. 1: Rozdíly mezi novým a tradičním terorismem .....	13
Tab. 2: Seznam největších teroristických útoků do roku 2018.....	22
Tab. 3: Útoky na měkké cíle na území ČR do roku 2016.....	33
Tab. 4: Otevírací doba VTP-ICT .....	49
Tab. 5: Otevírací doba Bamboo club .....	49
Tab. 6: Porovnání zlínské trestné činnosti s městy s podobným počtem obyvatel.....	51
Tab. 7: Studenti prezenční, anglické a kombinované formy bakalářského studia.....	62
Tab. 8: Studenti prezenční, anglické a kombinované formy magisterského studia.....	63
Tab. 9: Studenti prezenční, anglické a kombinované formy bakalářského studia.....	63
Tab. 10: Konkrétní pozice a počet akademických pracovníků na FAI v roce 2019...64	
Tab. 11: Charakteristika osob s oprávněným a řízeným vstupem v objektu U5 .....	67
Tab. 12: Klasifikace závažnosti .....	69
Tab. 13: Klasifikace odhalení .....	70
Tab. 14: Klasifikace výskytu .....	70
Tab. 15: FMEA referenčního objektu.....	71
Tab. 16: FMEA analýza s náležitým opatřením a mírou rizika po aplikování trvalého opatření.....	73
Tab. 17: Bodové hodnocení a charakteristika dostupnosti .....	83
Tab. 18: Bodové hodnocení a charakteristika složitosti .....	84
Tab. 19: Bodové hodnocení a charakteristika atraktivity .....	85
Tab. 20: Bodové hodnocení a charakteristika dopadu na životy .....	85
Tab. 21: Bodové hodnocení a charakteristika dopadu na společenství .....	86
Tab. 22: Určení dostupnosti, atraktivity a složitosti jednotlivých forem útoku .....	87
Tab. 23: Určení dopadu na životy a na společenství jednotlivých forem útoku.....	88
Tab. 24: Výsledná míra ohrožení jednotlivých forem útoku .....	89
Tab. 25: Celková míra ohrožení v závislosti na umístění a načasování útoku .....	90
Tab. 26: Návrh nápravných opatření teroristických útoků .....	92

## SEZNAM PŘÍLOH

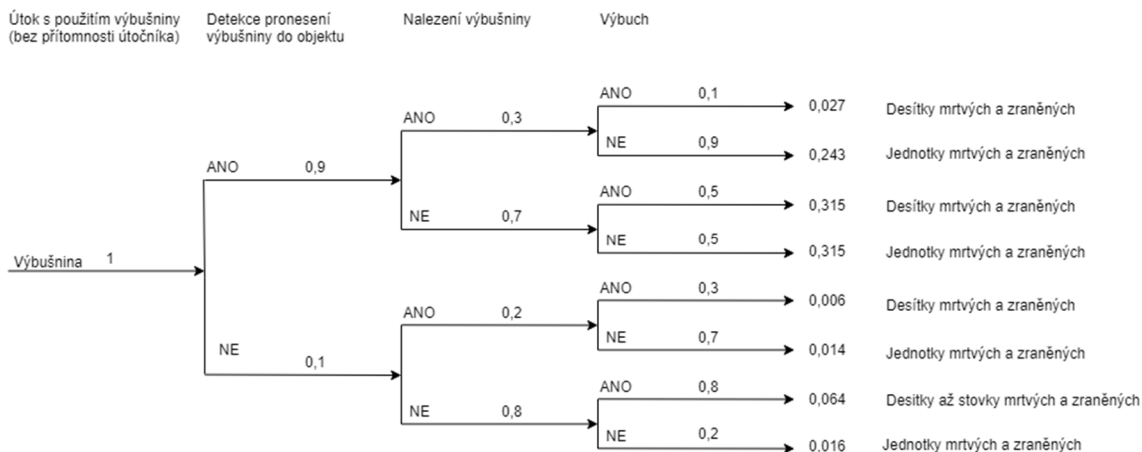
Příloha I      ETA analýzy nápravného opatření

Příloha II     Výpočty ohrožení v závislosti na lokalizaci a načasování útoku

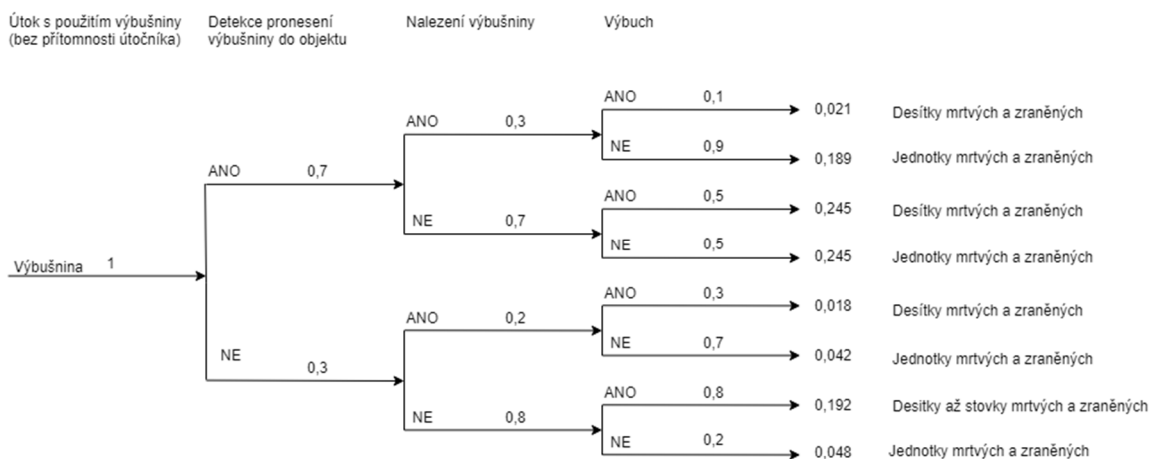
# PŘÍLOHA P I: TA ANALÝZY NÁPĚVNÉHO OPATŘENÍ

## 1. Útok s použitím výbušniny (bez přítomnosti útočnicka):

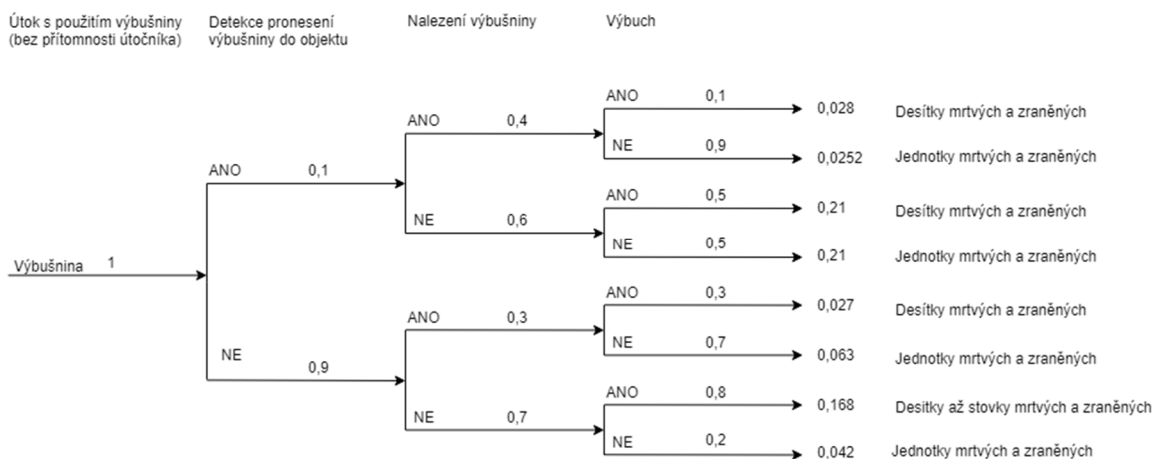
### Nápravné opatření 1: Detektor výbušnin:



### Nápravné opatření 2: Prohlídka podezřelých fyzickou ochranou – ostrahou

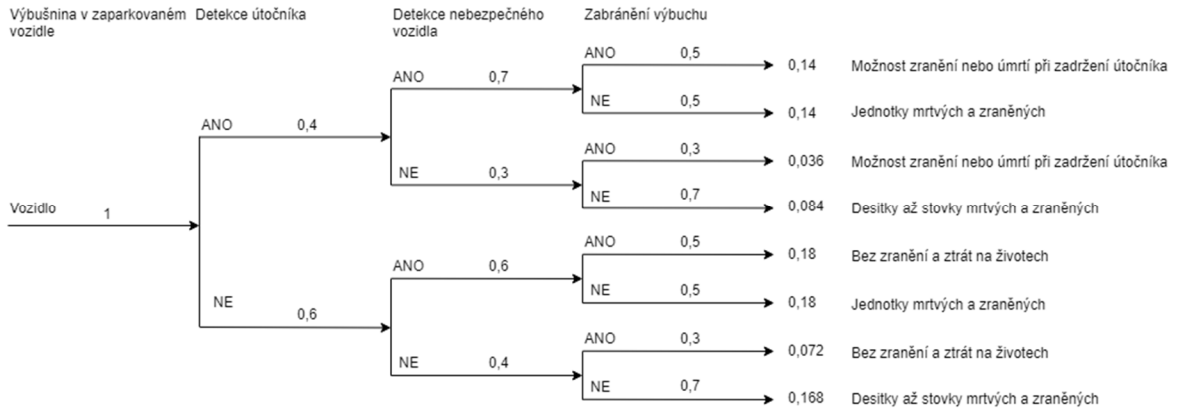


### Nápravné opatření 3: Pravidelné obchůzky

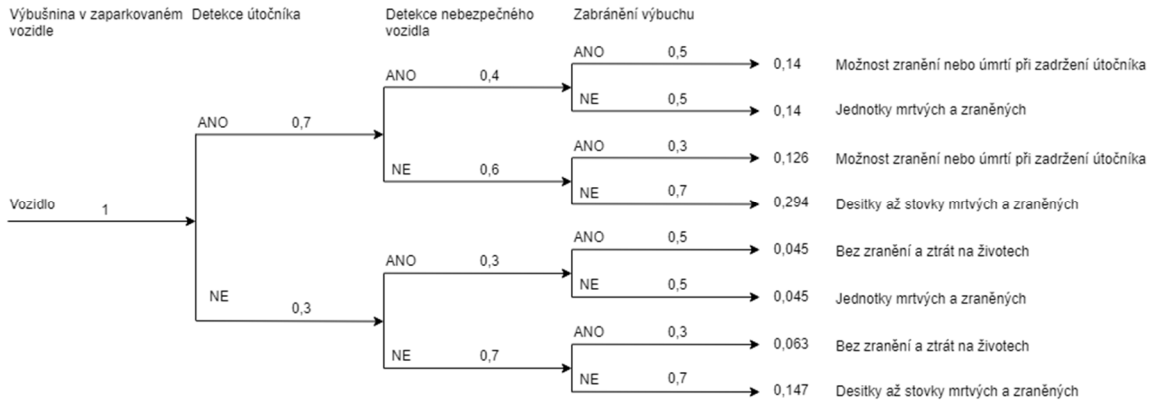


## 2. Výbušnina v zaparkovaném vozidle:

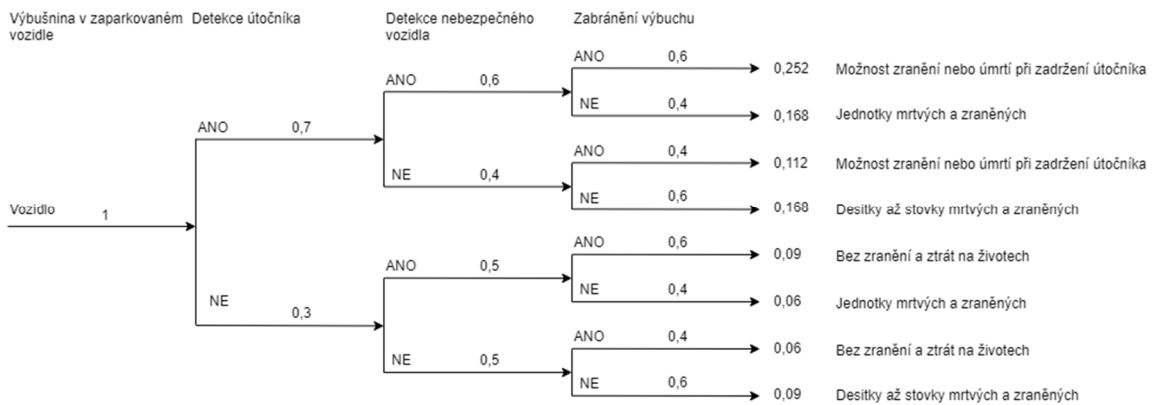
### Nápravné opatření 1 – Závora před parkovištěm pro zaměstnance



### Nápravné opatření 2 – Betonové sloupky

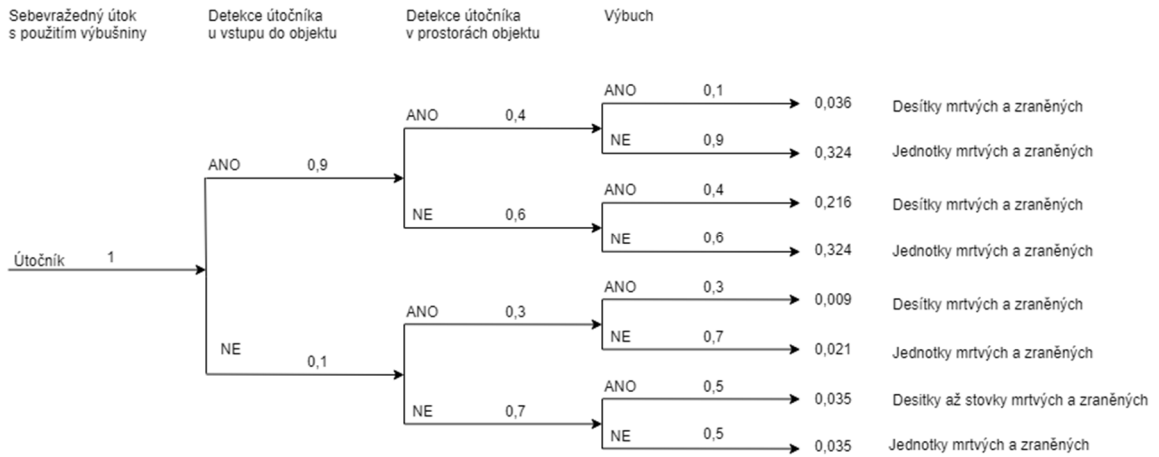


### Nápravné opatření 3 – Betonové zábrany:

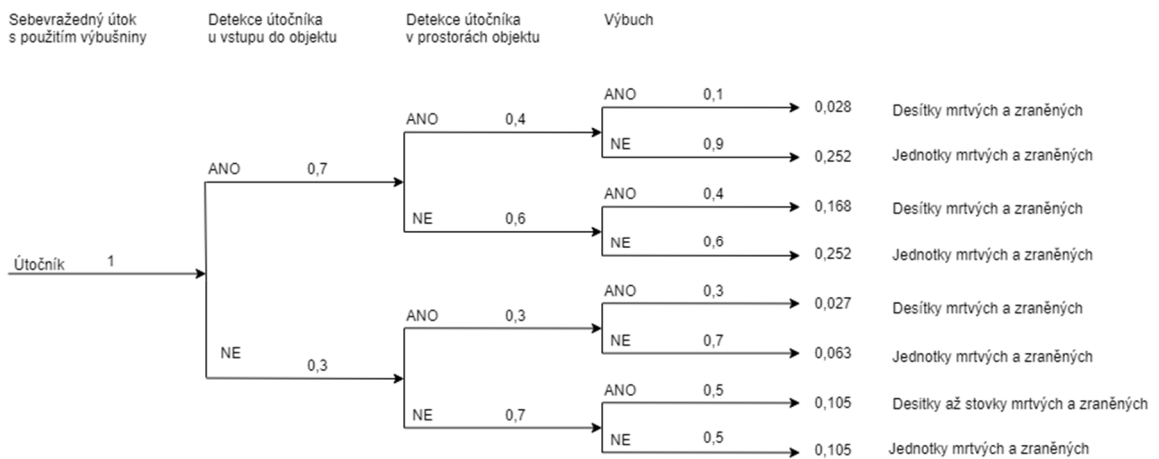


### 3. Sebevražedný útok s výbušninou:

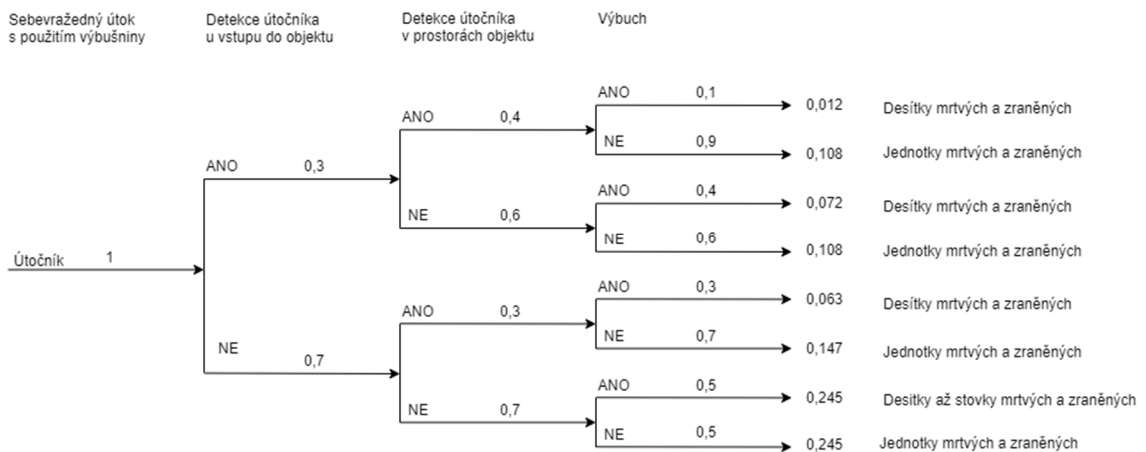
#### Nápravné opatření 1 – Detektor výbušnin:



#### Nápravné opatření 2 – Prohlídky podezřelých

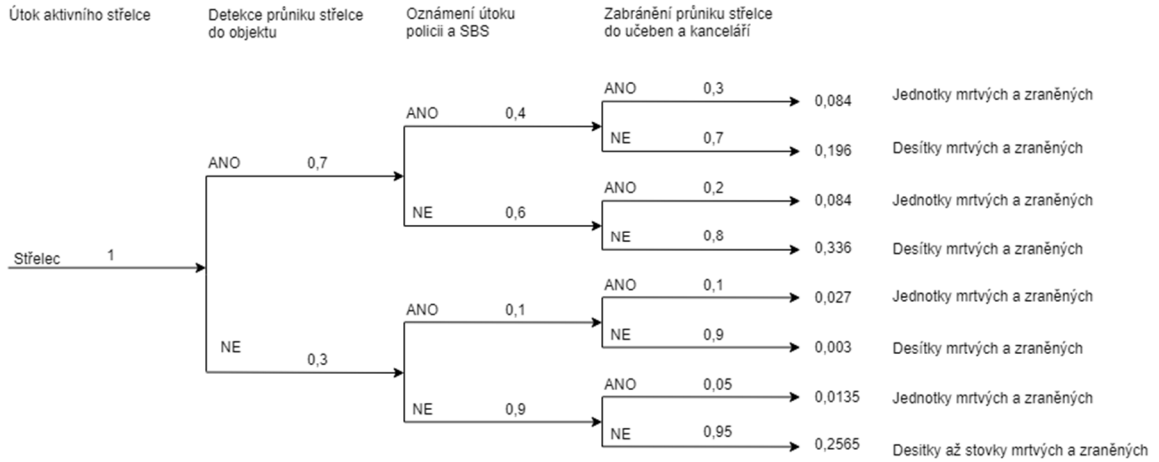


#### Nápravné opatření 3 – VSS

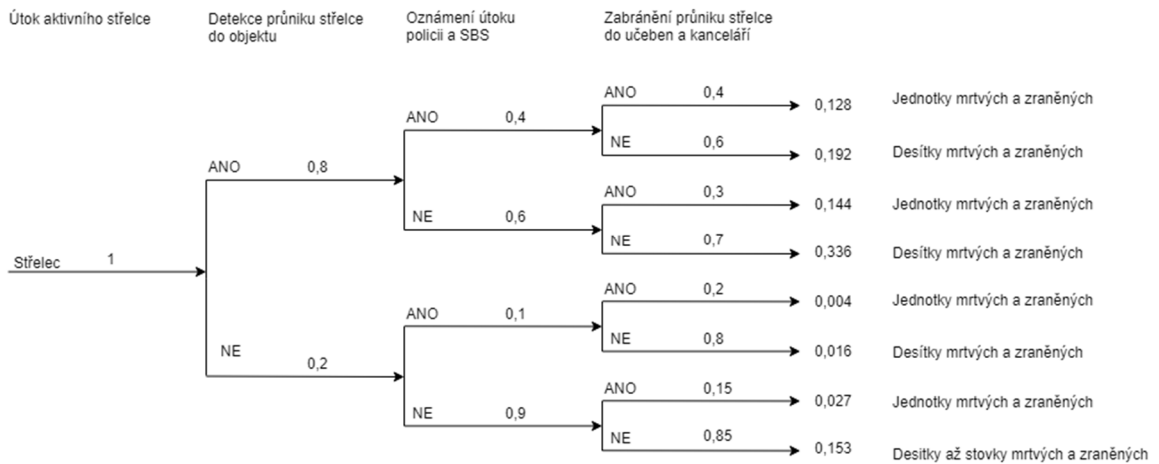


#### 4. Napadení střelnou zbraní:

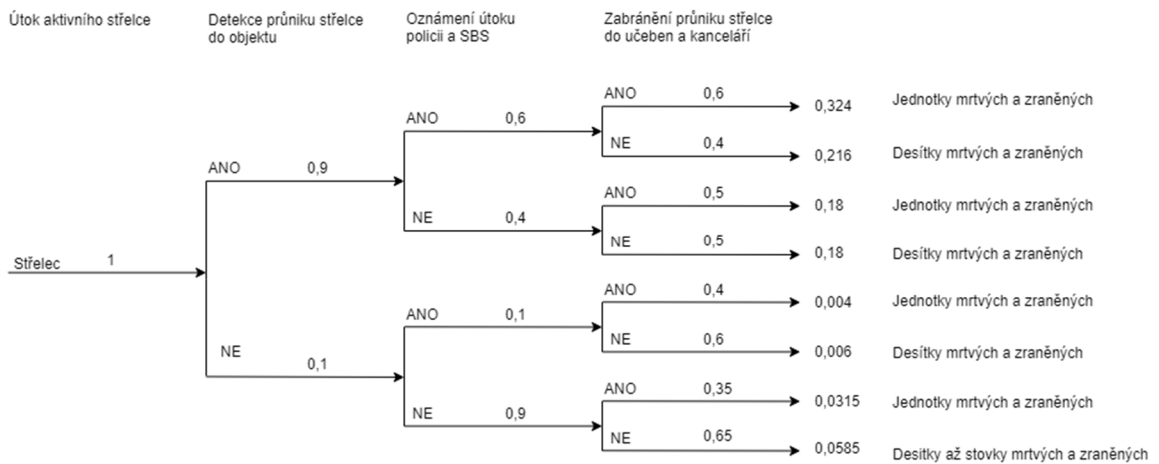
##### Nápravné opatření 1 – VSS



##### Nápravné opatření 2 – Ozbrojená ostraha



##### Nápravné opatření 3 – Rotační turnikety



## PŘÍLOHA P II: VÝPOČTY OHROŽENÍ V ZÁVISLOSTI NA LOKALIZACI A NAČASOVÁNÍ ÚTOKU

Tabulka výpočtu ohrožení v závislosti na lokalizaci útoku:

Útok	Lokalizace Ohrožení	
	V objektu	Před objektem
Napadení chladnou zbraní	180	119
Napadení střelnou zbraní	180	128
Žhářský útok	228	204
Braní rukojmí a barikádová situace	120	294
Výbušnina v poštovní zásilce	120	98
Sebevražedný útok s použitím výbušniny	130	96
Útok s použitím výbušniny (bez přítomnosti útoč- níka)	132	110
<b>Celkové ohrožení</b>	<b>1090</b>	<b>1049</b>

Tabulka výpočtu ohrožení v závislosti na denní době útoku:

Útok	Ohrožení v různé denní dobu	
	V době výuky	Mimo výuku
Napadení chladnou zbraní	299	x
Napadení střelnou zbraní	308	x
Žhářský útok	432	294
Braní rukojmí a barikádová situace	218	x
Výbušnina v poštovní zásilce	120	x
Sebevražedný útok s použitím výbušniny	226	x
Útok s použitím výbušniny (bez přítomnosti útoč- níka)	242	x
<b>Celkové ohrožení</b>	<b>1845</b>	<b>294</b>