Užití procesního inženýrství v kybernetické bezpečnosti

Žaneta Pěrková

Bakalářská práce
2018

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav krizového řízení
akademický rok: 2017/2018

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

Jméno a příjmení:	**Žaneta Pěrková**
Osobní číslo:	**L15054**
Studijní program:	**B3909 Procesní inženýrství**
Studijní obor:	**Ovládání rizik**
Forma studia:	**prezenční**

Téma práce: **Užití procesního inženýrství v kybernetické bezpečnosti**

Zásady pro vypracování:

1. **Analyzujte informační zdroje.**
2. **Vyjádřete odpovídající část požadovaného modelu.**
3. **Vyhodnoťte kriteria procesů vhodným modelováním.**
4. **Navrhněte řešení procesů z hlediska kybernetické bezpečnosti.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

[1] PORADA, Viktor. Kriminalistika: technické, forenzní a kybernetické aspekty. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2016. ISBN 978-80-7380-589-0.

[2] HRŮZA, Petr. Kybernetická bezpečnost II. Vyd. 1. Brno: Univerzita obrany, 2013, 100 s. ISBN 978-80-7231-931-2

[3] ŠEFČÍK, Vladimír a Jiří KONEČNÝ. Procesní inženýrství: bezpečné a spolehlivé vedení procesů. Vyd. 1. Ve Zlíně: Univerzita Tomáše Bati, 2013, 106 s. ISBN 978-80-7454-280-0

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **prof. Ing. Jiří Dvořák, DrSc.**
Ústav krizového řízení

Datum zadání bakalářské práce: **3. listopadu 2017**

Termín odevzdání bakalářské práce: **15. května 2018**

V Uherském Hradišti dne 10. listopadu 2017

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta logistiky a krizového řízení

L.S.

doc. RNDr. Jiří Dostál, CSc.
děkan

Ing. et Ing. Jiří Konečný, Ph.D.
ředitel ústavu

PROHLÁŠENÍ AUTORA
BAKALÁŘSKÉ / DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

- odevzdáním bakalářské/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[1)];
- bakalářská/diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji bakalářskou/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[2)];
- podle § 60[3)] odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60[3)] odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou/diplomovou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské/diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské/diplomové práce využít ke komerčním účelům;
- pokud je výstupem bakalářské/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 bakalářské/diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti 11.5.2018

podpis studenta

1) zákon č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, § 47b Zveřejňování závěrečných prací:

(1) Vysoká škola nevýdělečně zveřejňuje bakalářské, diplomové, disertační a rigorózní práce, u kterých proběhla obhajoba, včetně posudků oponentů a výsledku obhajoby prostřednictvím databáze kvalifikačních prací, kterou spravuje. Způsob zveřejnění stanoví vnitřní předpis vysoké školy. Vysoká škola disertační práce nezveřejňuje, byla-li již zveřejněna jiným způsobem.

(2) Bakalářské, diplomové, disertační a rigorózní práce odevzdané uchazečem k obhajobě musí být též nejméně pět pracovních dnů před konáním obhajoby zveřejněny k nahlížení veřejnosti v místě určeném vnitřním předpisem vysoké školy nebo není-li tak určeno, v místě pracoviště vysoké školy, kde se má konat obhajoba práce. Každý si může ze zveřejněné práce pořizovat na své náklady výpisy, opisy nebo rozmnoženiny.

(3) Platí, že odevzdáním práce autor souhlasí se zveřejněním své práce podle tohoto zákona, bez ohledu na výsledek obhajoby.

(4) Vysoká škola může odložit zveřejnění bakalářské, diplomové, disertační a rigorózní práce nebo jejich části, a to po dobu trvání překážky pro zveřejnění, nejdéle však na dobu 3 let. Informace o odložení zveřejnění musí být spolu s odůvodněním zveřejněna na stejném místě, kde jsou zveřejňovány bakalářské, diplomové, disertační a rigorózní práce, jíž se týká odklad zveřejnění podle věty první, jeden výtisk práce k uchování ministerstvu.

2) 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, § 35 odst. 3:

(3) Do práva autorského také nezasahuje škola nebo školské či vzdělávací zařízení, užije-li nikoli za účelem přímého nebo nepřímého hospodářského nebo obchodního prospěchu k výuce nebo k vlastní vnitřní potřebě dílo vytvořené žákem nebo studentem ke splnění školních nebo studijních povinností vyplývajících z jeho právního vztahu ke škole nebo školskému či vzdělávacího zařízení (školní dílo).

3) 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, § 60 Školní dílo:

(1) Škola nebo školské či vzdělávací zařízení mají za obvyklých podmínek právo na uzavření licenční smlouvy o užití školního díla (§ 35 odst. 3). Odpírá-li autor takového díla udělit svolení bez vážného důvodu, mohou se tyto osoby domáhat nahrazení chybějícího projevu jeho vůle u soudu. Ustanovení § 35 odst. 3 zůstává nedotčeno.

(2) Není-li sjednáno jinak, může autor školního díla své dílo užít či poskytnout jinému licenci, není-li to v rozporu s oprávněnými zájmy školy nebo školského či vzdělávacího zařízení.

(3) Škola nebo školské či vzdělávací zařízení jsou oprávněny požadovat, aby jim autor školního díla z výdělku jím dosaženého v souvislosti s užitím díla či poskytnutím licence podle odstavce 2 přiměřeně přispěl na úhradu nákladů, které na vytvoření díla vynaložily, a to podle okolností až do jejich skutečné výše; přitom se přihlédne k výši výdělku dosaženého školou nebo školským či vzdělávacím zařízením z užití školního díla podle odstavce 1.

ABSTRAKT

Tato práce řeší problematiku užití procesního inženýrství v kybernetické bezpečnosti na konkrétním příkladu, kterým je kybernetický útok na automobil. K řešení této problematiky bylo využito metod modelování procesů a dotazníkového šetření. Byl vytvořen model vhodný pro kybernetickou bezpečnost a upozornil, že touto problematikou by se měli lidé více zabývat a to zejména v rámci vlastního bezpečí.

Klíčová slova:

Proces, Procesní inženýrství, Model, Kyberprostor, Kybernetická bezpečnost

ABSTRACT

This work sloves the problem of the use of process engineering in cyber specific example, which is a cyber attack to an automobile. Methods of modeling processes and questionnaire investigations were used to solvet his problem. A model suitable for cybersecurity has been developed and pointed out that this is sue should be more dealt by people, especially within thein own safety.

Keywords:

Processes, Process Engineering, Model, Cyberspace, CyberSecurity

Mé velké díky patří mému vedoucímu bakalářské práce prof. Ing. Jiřímu Dvořákovi, DrSc. za jeho vstřícný přístup, cenné rady, trpělivost, důvěru a čas, který mi věnoval. Dále pak bych ráda poděkovala všem, kteří byli jakýmkoli způsobem angažovaní při řešení mé bakalářské práce a konkrétně Ing. Pavlu Ondrovi za jeho čas a poskytnuté konzultace.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

I TEORETICKÁ ČÁST 11
1 ANALÝZA INFORMAČNÍCH ZDROJŮ 12
1.1 VYMEZENÍ ZÁKLADNÍCH POJMŮ 13
1.1.1 Proces 13
1.1.2 Procesní inženýrství 14
1.1.3 Model 17
1.1.4 Bezpečnost 17
1.1.5 Kyberprostor 17
1.1.6 Kybernetická bezpečnost 17
1.1.7 Multimediální systémy v automobilu 18
1.1.8 Bezklíčový přístup k automobilu 18
1.1.9 Firmware 19
1.1.10 ECU –Engine Control Unit, centrální elektronická řídící jednotka 19
1.1.11 Sběrnice CAN (Controller Area Network) 19
2 VYJÁDŘENÍ MODELU 20
2.1 TVORBA MODELU 20
2.1.1 Model procesů pro uvažovaný kyberprostor 21
2.1.2 Model pro kybernetickou bezpečnost 21
2.1.3 Model pro řešení procesů 21
2.2 MOŽNOSTI MODELOVÁNÍ 22
2.3 VÝZKUM POMOCÍ DOTAZNÍKOVÉHO ŠETŘENÍ 24
II PRAKTICKÁ ČÁST 26
3 VYHODNOCENÍ KRITÉRIÍ PROCESŮ MODELOVÁNÍM 27
3.1 DOTAZNÍKOVÉ ŠETŘENÍ 27
3.1.1 Dosažené výsledky 27
Testování nezávislosti mezi rizikovostí a pohlavím 31
Testování nezávislosti mezi rizikovostí a věkem 34
3.2 VOLBA KRITÉRIÍ PROCESU A JEJICH HODNOCENÍ 37
3.2.1 Stáří automobilu 37
3.2.2 Čas potřebný k napadení vozidla: 37
3.2.3 Technické vybavení potřebné k napadení vozidla: 38
3.3 VYHODNOCENÍ KRITÉRIÍ PROCESU 39
4 NÁVRH PROCESŮ Z HLEDISKA KYBERNETICKÉ BEZPEČNOSTI 43
4.1 NÁVRH ŘEŠENÍ PRO MODEL PROCESU KYBERNETICKÉHO ÚTOKU NA SYSTÉM ZAMYKÁNÍ A ODEMYKÁNÍ AUTOMOBILU 43
4.2 NÁVRH ŘEŠENÍ PRO MODEL PROCESU KYBERNETICKÉHO ÚTOKU NA SYSTÉMY V AUTOMOBILU 43
ZÁVĚR 46
SEZNAM POUŽITÉ LITERATURY 49
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK 54
SEZNAM OBRÁZKŮ 55
SEZNAM TABULEK 56
SEZNAM PŘÍLOH 57

ÚVOD

V dnešní době se postupně stávají čím dál více frekventované pojmy procesní inženýrství, kybernetická bezpečnost, kybernetické útoky a modelování procesů v kybernetické válce apod. Tématem této práce je užití procesního inženýrství v kybernetické bezpečnosti. Protože se procesní inženýrství promítá do mnoha oblastí, je možné u každé oblasti specifikovat její kybernetickou bezpečnost.V této práci se konkrétně zaměříme na oblast automobilového průmyslu, protože riziko kybernetických útoků na automobil se díky moderním technologiím neustále zvyšuje. Do podvědomí společnosti se problematika kybernetických útoků na automobil dostala pravděpodobně kolem roku 2013. Tehdy se Charlie Miller a Chris Valasek (2015) pokusili o napadení systémů ve vozidle Toyota Prius, přímým napojením na řídící jednotku. Jejich pokus byl úspěšný a na základě toho se rozhodli provést další pokus. Tentokrát se zaměřili na kybernetický útok na multimediální systém v tehdy nově vyrobeném automobilu Jeep Cherokee. [13] I tento pokus o napadení multimediální systému byl úspěšný.

Když se v roce 2015 dotázal americký senátor Edward Markey asi dvaceti výrobců automobilů jestli jsou jejich auta proti takovým útokům chráněna, 16 jich odpovědělo, že ne. [6] Z toho vyplývá, že kybernetickou bezpečnost v nově vyrobených vozech s multimediálními systémy, neřeší 80% dotazovaných výrobců automobilů. Podle současných odborných článků však řešení této problematiky, tak trochu utichá. Výrobci automobilů se zřejmě domnívají, že tyto útoky nejsou tolik pravděpodobné, a proto se stále zaměřují více na komfort, design a jízdní vlastnosti automobilů, než na ochranu svých multimediálních systémů. Hlavním cílem této práce proto bude vytvoření modelu dvou procesů napadení automobilu útočníkem. Konkrétně se zaměříme na proces kybernetického útoku na systém zamykání a odemykání automobilu a proces kybernetického útoku na multimediální systém v automobilu. Dílčími cíli práce bude zjistit, jaké je povědomí společnosti o možnosti kybernetického útoku na automobil, hodnocení rizikovosti daného útoku a návrh, jak procesy ošetřit z hlediska kybernetické bezpečnosti.

Pro přehlednost nyní krátce popíšeme strukturu předkládané práce. V první kapitole popíšeme analyzované informační zdroje. V části této kapitoly vymezíme základní teoretické koncepty, se kterými budeme operovat v průběhu celé bakalářské práce. Nejdříve vysvětlíme, co je proces, popíšeme procesní inženýrství, definujeme kyberprostor a přiblížíme

koncept kybernetické bezpečnosti. Dále je v této kapitole přehled knih, internetových zdrojů a konferencí, které se věnují námi řešenému tématu. Druhá kapitola popíše tvorbu modelu. Zahrnuje konkrétní popis modelu procesů pro uvažovaný kyberprostor, kybernetickou bezpečnost a model řešení procesů. Seznámí čtenáře s možnostmi modelování a postupem tvorby dotazníkového šetření.

Praktická část nejdříve popíše dotazníkové šetření, které bude zaměřeno na běžné uživatele osobních automobilů. Zajímat nás bude především závislost různých proměnných na hodnocení rizik spojených s kybernetickým útokem. Aplikace systémového vyjádření vybraných a definovaných pojmů procesního inženýrství v kybernetické bezpečnosti na konkrétních modelech je uvedená v praktické části v kapitole třetí a to na příkladu kybernetického útoku na automobil. Možností kybernetického útoku na automobil je více, ovšem my se zaměříme pouze na dva nejčastější. Jsou jimi pro tuto práci kybernetický útok na systém zamykání a odemykání automobilu a kybernetický útok na multimediální systémy v automobilu, skrze které může dojít k absolutnímu ovládnutí vozidla útočníkem.

Poslední kapitola práce řeší návrhy procesů z hlediska kybernetické bezpečnosti. Pro každý z procesů navrhneme způsob zabezpečení tak, aby k těmto kybernetickým útokům nedocházelo nebo aby byla práce útočníků dostatečně ztížena. Předkládaná práce si neklade za cíl pokrýt téma v celé jeho šíři. Spíše chce představit dosud méně zkoumanou problematiku a tím částečně seznámit akademickou obec dalšími možnostmi a výzvami, které nás v této oblasti čekají.

I. TEORETICKÁ ČÁST

1 ANALÝZA INFORMAČNÍCH ZDROJŮ

Na začátku naší práce jsme vyhledávali informace o základních konceptech, kterými jsou pro nás procesní inženýrství a kybernetická bezpečnost. Při hledání jsme vycházeli z několika informačních zdrojů. Hledali jsme jak na internetu pomocí internetového vyhledávače Google, respektive GoogleBooks, tak i v literatuře.

Kybernetická bezpečnost je velmi aktuální a diskutované téma, proto se v internetovém vyhledávači při zadání tohoto pojmu zobrazí nesčetné množství odkazů, ze kterých jsme čerpali potřebné informace do této práce. Ne všechny tyto zdroje ovšem byly ověřitelné a použitelné, proto jsme do naší práce vybrali jen některé odborné konference a reálné příklady.

Každoročně se pořádá několik konferencí na téma kybernetická bezpečnost a okolnosti s ní související. Aktuální přehled konferencí pro rok 2018 napříč celým světem můžeme nalézt na webu InfoSec Conferences. S touto prací souvisí populární konference Black Hat, která proběhla v roce 2015 v Las Vegas, o úspěšnosti této konference svědčí minimálně to, že v letošním roce proběhne její již 21.ročník. Podobné konference probíhají i v České republice. Zde uvádíme výčet několika konferencí z českého prostředí:

- Cíl a cesta ke kybernetické bezpečnosti nejen v mezích zákona v roce 2015 v Brně
- Bezpečnostní konferenci ČABM v roce 2016 v Mikulově
- Konference o kybernetické bezpečnosti v roce 2017 v Praze
- Ukrajina a konference o kybernetické bezpečnosti státu v roce 2017 v Praze
- na podzim roku 2018 je plánovaná konference s názvem Řízení procesů a aplikace moderních technologií – Kybernetická bezpečnost

Na téma kybernetické bezpečnosti jsme narazili i v médiích, a to konkrétně v periodicích zaměřených na IT, případně přímo na automobilový průmysl. Například časopis Automa, který vychází v tištěné podobě i na internetu, se ve svém článku zmiňuje o Konferenci o kybernetické bezpečnosti a smart grids, která proběhla na podzim 2011 v Amsterdamu. Ve svém online magazínu číslo 11-12/2016 vydal ICT NETWORK *NEWS* článek o Kybernetické bezpečnosti a vizi do roku 2017. Časopis IT Systems vydalv roce 2017 online článek s názvem *Vím, že nic nevím - pro kybernetickou bezpečnost bohužel platí známé Sokratovo úsloví*.

Internetových časopisů, které se ve svých článcích zmiňují o kybernetické bezpečnosti je nepřeberné množství, vybrali jsme ale pouze některé, které se přímo vztahují k tématu naší práce. Jejich přímé odkazy přikládám do příloh (Příloha PI) bakalářské práce.

Co se týče vydané české literatury, čerpali jsme především ze dvou titulů. *Kybernetická bezpečnost II* od Petra Hrůzy a *Kybernetická bezpečnost: teorie a praxe* od Martina Hromady. Dále jsme nahlédli do knihy, která tuto problematiku řeší z hlediska kriminalistiky - Kriminalistika: Technické, forenzní a kybernetické aspekty od Viktora Porady. Zahraniční literatura je na toto téma o něco bohatší než ta česká, jako příklad bych uvedla knihu od Petera W. Singera a Allana Friedmana *Cybersecurity: What Everyone Needs to Know* nebo také knihy od Lina –Choi *Cybersecurity and Homeland Security* a George K. Kostopoulose: *Cyberspace and Cybersecurity.*

Pokud se zaměříme na zdroje informací o procesním inženýrství, je jich podstatně méně než zdrojů, které se týkají kybernetické bezpečnosti. Primární literatura, ze které jsme čerpali informace je *Procesní inženýrství bezpečné a spolehlivé vedení procesů* od autorů Vladimíra Šefčíka a Jiřího Konečného. Dále to byli samozřejmě internetové zdroje uvedené v příloze práce (příloha PI). Konference, kde je mimo jiné zmínka o procesním inženýrství, se pořádá už po několik let a její celý název zní Konference chemického a procesního inženýrství CHISA.

1.1 Vymezení základních pojmů

V této kapitole definujeme základní pojmy a další pojmy k objasnění problematiky. Tento krok je nezbytný k dalšímu navázání na následující kapitoly této práce, ve kterých budeme pojmy používat ve tvorbě samotných modelů.

1.1.1 Proces

Proces je všeobecně v mnoha publikacích a napříč mnoha odvětvími popisován jako soubor činností, které mají za úkol přeměnu vstupů na výstupy za řízených podmínek. Každý proces je jinak složitý. Složitost procesu ovlivňuje počet úloh a vzájemných souvislostí, které v jeho průběhu nastanou. Odvětví, ve kterých můžeme definici procesu nalézt,je hned několik, například v informatika, matematika, chemie a biologie, psychologie apod.

Charakteristickými rysy procesu mohou být vstup, za který považujeme příčinu zahájení procesu, výstup, který se zároveň bere i jako cíl procesu, aktivita, role a zdroje procesu. [35]

Obr.1. Znázornění procesu, (Vlastní zpracování)

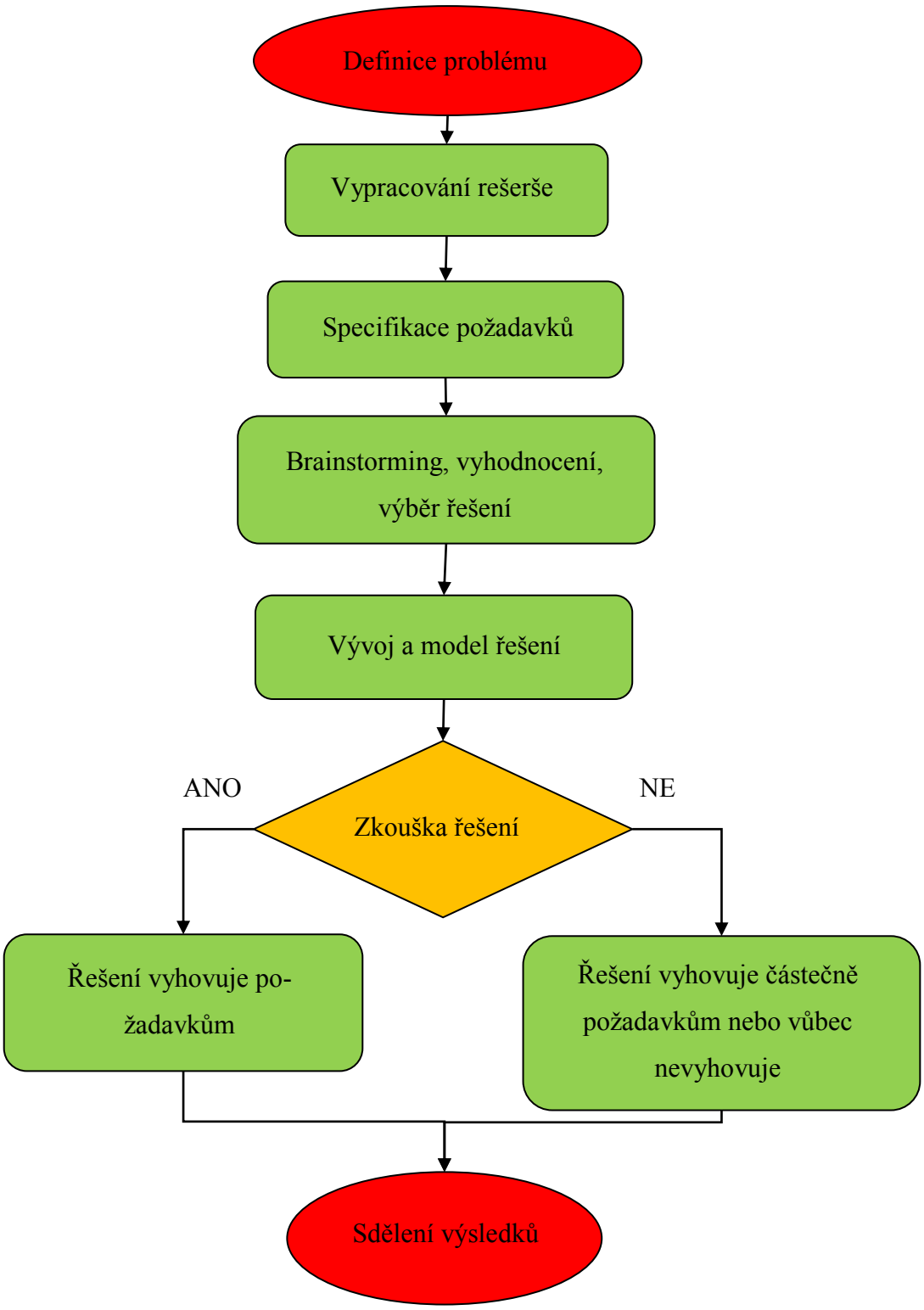
1.1.2 Procesní inženýrství

Pro procesní inženýrství je specifické široké spektrum působnosti. Jeho náplní je vývoj procesů, optimální vedení procesů, navrhování procesů a jejich promítání. Konkrétně můžeme jmenovat několik oblastí působnosti procesního inženýrství. Jedná se například o řízení procesů v oblasti ekonomiky, kde se řeší ekonomické aspekty, jako jsou cena a celkové náklady. V oblasti energetiky je účelem řízení procesů minimalizace spotřeby energie a škodlivých emisí, dále může procesní inženýrství také působit na oblast potravinářského a farmaceutického průmyslu nebo na průmysl zpracování ropy a zemního plynu. Jako poslední oblast můžeme zmínit ochranu životního prostředí, kde se řízení procesů promítá do čistíren odpadních vod, termického a netermického zneškodňování odpadů. V této práci vyjádříme promítnutí procesního inženýrství do oblasti kybernetické bezpečnosti.

Procesní inženýr vytváří, vyvíjí, zavádí a monitoruje zařízení nebo procesy ve výrobním procesu. Spolupráce s lidmi na výrobním systému, výzkumu a vývoji je výsledkem konání procesních inženýrů.Předpokladem proto, aby člověk mohl tuto práci vykonávat, je bakalářské studium v příbuzném oboru, manažerské zkušenosti nebo obchodní kvalifikace. Také jsou tu vlastnosti, které by měl procesní inženýr mít, například se jedná o komunikační schopnosti, schopnost umět řešit problémy s klidem i když je pod tlakem, mít obchodní povědomí, kritické a logické myšlení, počítačové dovednosti, analytické dovednosti, a jiné. [39]

Na obrázku (Obr.2) jsme pomocí vývojového diagramu znázornili přístup k procesnímu inženýrství. Na samém počátku je definice problému, který je potřeba řešit. Následuje vypracování rešerše a specifikace požadavků na definovaný problém. V dalším kroku je

vhodné provést brainstorming, z něj vyhodnotit problém a vybrat jeho vhodné řešení. Model problému a jeho řešení je další fází. Následuje zkouška zvoleného řešení, zde se nabízí dvě varianty - zkouška bude nebo nebude úspěšná. V obou případech končí celý proces sdělením výsledků.



Obr.2. Vývojový diagram přístupu k procesnímu inženýrství, (Vlastní zpracování)

1.1.3 Model

Každý originál lze nahradit jeho obrazem. Originál lze zjednodušit právě tak, že vytvoříme model, ve kterém budou zahrnuty pouze jeho podstatné vlastnosti. Prostředky používané k popisu jsou například rovnice, schémata, vývojové diagramy a mnoho dalších. Výhody sestavování modelů jsou cena, opakované použití nebo předpověď neznámých vlastností daného originálu.[26]

1.1.4 Bezpečnost

Samotný pojem bezpečnost není přesně definován. Dokonce ani zákon nám tento pojem přesně nedefinuje. Skoro v každé literatuře najdeme jinou, avšak velmi obdobnou definici tohoto pojmu. Zjednodušeně by se proto dala bezpečnost popsat jako stav, kdy dochází k vyloučení nebo odstranění jakýchkoli hrozeb pro daný objekt a jeho zájmy. Tyto hrozby jsou eliminovány na co nejnižší úroveň, protože je objekt proti nim vybaven.[31]

1.1.5 Kyberprostor

Pojem kyberprostor se může na první pohled zdát poněkud nový, avšak jeho definice je známá již třicet let. Petr Hrůza pojem kyberprostor popisuje jako: „*Virtuální svět vytvořený moderními technologickými prostředky, v němž se informace vytvářejí, zpracovávají, ukládají a šíří pomocí elektromagnetického vlnění.“[14]*

Nejčastěji v nás pojem kyberprostor může vyvolávat dojem nějakého internetového prostředí, ale není tomu tak. I v případě, že je člověk „off-line“ může být vystaven hrozbě nákazy například fyzickými nosiči (např. USB flash disky, SD karty atd.)[41]

1.1.6 Kybernetická bezpečnost

Kybernetickou bezpečností chápeme soubor opatření, která mají právní, organizační, technický a fyzický charakter. Tato opatření mají za cíl čelit kybernetickým útokům. Pokud takové útoky nastanou, je jejich další funkcí zmírňovat nebo napravovat následky těchto útoků. Jedním z hlavních poslání kybernetické bezpečnosti je ochrana před krádeží identity.

Legislativně je kybernetická bezpečnost ukotvena v několika ISO a IEC normách. ISO představuje Mezinárodní organizaci pro normalizaci a IEC je Mezinárodní elektrotechnická komise. Celosvětově bylo vydáno několik dokumentů a koncepcí v souvislosti

s kybernetickou ochranou. V České republice je zřízeno Národní centrum kybernetické bezpečnosti a od roku 2014 je v platnosti Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

Nejznámější kybernetické útoky v posledních letech byly například dálkové vypnutí internetových sítí administrativy a státních podniků v Estonsku v roce 2007, útoky na weby a webová sídla v Gruzii v roce 2008, napadení SCADA systémů červem Stuxnet v Iránu v roce 2010, o rok později neminul útok ani USA v podobě zničení čerpadla v síti veřejných vodovodů a ten samý rok v Jižní Koreji hackeři napadli na 40 webových stránek vládních a dalších institucí.[14]

Velká vlna kybernetických útoků postupovala v loňském roce 2017 přes Rusko, Ukrajinu až do Evropy, napaden byl například ruský ropný gigant, banky a vládní počítače, letiště na Ukrajině, francouzská stavební firma či antivirové společnosti.[33]

Nejaktuálnější útok většího charakteru proběhl letos na zimní olympiádě v Koreji. Během slavnostního ceremoniálu bylo zasaženo televizní vysílání a přístup k internetu.[24]

1.1.7 Multimediální systémy v automobilu

Toto zařízení je v automobilu nejčastěji umísťováno na přístrojové desce mezi řidičem a spolujezdcem. Tento systém je obvykle vybaven navigací GPS, informacemi o stavu vozidla a průběhu jízdy. Multimediální systém zajišťuje komunikaci řidiče s okolním světem. Ve většině případů je možnost připojení na internet. Mimo jiné lze tímto systémem zobrazit diagnostické informace nebo měnit nastavení vozidla.[25] Nejznámější multimediální systémy používané výrobci automobilů jsou například systém MMI od Audi, systém iDrive od BMW nebo Mercedes Me connect.[4] Všechny uvedené systémy jsou téměř ve všem totožné, liší se nanejvýš svým designem.

1.1.8 Bezklíčový přístup k automobilu

Systém se označuje jako KESSY(tzn. Keyless Entry, Start and Exit System). Česky bychom to volně přeložili jako bezklíčový vstup, bezklíčové startování a bezklíčové uzamčení automobilu. Automobiloví výrobci jej u moderních automobilů zavádějí proto, aby zvýšili komfort řidiče. Ve zkratce jde o celkový bezklíčový přístup do automobilu. Na předních dveřích automobilu se na vnější stranu kliky a do víka zavazadlového prostoru umísťuje dotykové čidlo. Pro zamknutí a odemknutí vozu poté stačí jen dotyk na umístěné či-

dlo. Úplně postačí, když bude mít majitel vozidla klíč na dálkové ovládání někde v blízkosti vozu, ať už jej má v oblečení nebo v příručním zavazadle. Další funkcí bezklíčového přístupu je startování a vypnutí motoru vozu.[17]

1.1.9 Firmware

„Software, na základě kterého může určité zařízení fungovat. Firmware se vztahuje k jednotlivým komponentám, jako je například harddisk, základní deska nebo i procesor. Je to tedy něco jako ovladač, který je potřeba pro chod zařízení.“[11]

1.1.10 ECU –Engine Control Unit, centrální elektronická řídící jednotka

„Jedná se o procesory řízený počítač, který zajišťuje chod dané funkce automobilu. Vlastní řídící jednotku mají například motor, airbagy, posilovač řízení, klimatizace, ABS, imobilizér, automatická převodovka a mnoho dalších.“[8]

1.1.11 Sběrnice CAN (Controller Area Network)

„Sběrnice dat elektronických řídících jednotek vozidla. Zajišťuje vzájemnou komunikaci mezi řídícími jednotkami. Na CAN-Bus je u moderních automobilů napojena prakticky celá elektronická soustava (například sledování otáček, vstřikování paliva, zapalování, katalyzátoru, ABS a další). Rychlým propojováním dat je dosaženo souhry všech elektronických komponentů sloužících například k automatickému zamknutí vozu, vypínání vnitřního osvětlení po určité prodlevě, signalizace při zjištění problémů, atd. Další kontrolní funkce systému CAN-Bus se vztahují také k motoru, klimatizaci, tempomatu nebo bezpečnostním prvkům.“[28]

2 VYJÁDŘENÍ MODELU

V této kapitole popíšeme proces tvorby konkrétních modelů pro integraci procesního inženýrství a kybernetické bezpečnosti. Dále také vysvětlíme postup tvorby modelu, jeho rozdělení a způsoby jakými lze modelovat. Tato kapitola také teoreticky popisuje postup výzkumu dotazníkového šetření, které jsme v další části práce využili k zjištění doplňujících dat.

2.1 Tvorba modelu

Před samotnou tvorbou modelu je důležité si definovat samotný systém. Je to abstrakce, kterou člověk využívá při analýze reálného prostředí jako nástroj k poznání reálných objektů nebo také logické a matematické konstrukce. Tyto abstrakce nám v procesu poznávání zobrazují systémové vlastnosti objektu a jevy vnějšího světa. V matematickém pojetí jsou to objekty, které se skládají z množin, prvků a vztahů mezi nimi. Při tvorbě modelu systému, je nutné zajistit, aby byl systém oddělen od svého okolí a nenastala situace, kdy by model svými výstupy ovlivňoval skrze okolí své vstupy.[7]

Pro tvorbu modelu se většinou využívá umělý, konkrétně matematický jazyk a jeho výrazové prostředky. Těmito prostředky mohou být např. graf a matice.

Pojem model jsme již definovali v předchozí kapitole. Nyní ještě doplníme rozdělení modelů. Modely lze podle své podstaty rozdělit do dvou skupin:

a) fyzický (fyzikální) model

Tento model můžeme definovat na základě fyzikální nebo geometrické podobnosti mezi modelovaným systémem a modelem. Jeho název vychází hlavně z faktu, že model je hmatatelný.

b) matematický model

Možnost zkoumat jevy na originálu, pomocí matematického popisu jejich průběhu, je hlavním znakem matematického modelu. Další vlastností modelu je jeho abstrakce. Informaci, kterou potřebujeme, získáme až řešením tohoto modelu.

Modelování představuje experimentální proces, při němž se zkoumanému objektu, kterým může být reálný objekt, dílo nebo stroj, přiřadí za určitých kritérií fyzický nebo abstraktní model. Podle toho, jak přiřadíme model k originálu, můžeme rozlišit způsoby modelování.

Vycházet můžeme z podobnosti modelu, což je jednoznačné vzájemné přiřazení vlastností, struktury a chování. Pokud se tedy budeme zabývat podobností modelu, existují 3 typy: *fyzikální, matematická* a *kybernetická*. Fyzikální podobnost určujeme na základě geometrické podobnosti parametrů a stavových veličin. O matematické podobnosti pojednáváme v případě, že jde o stejný matematický popis modelu a originálu. Kybernetická podobnost úzce souvisí s matematickou podobností, která se nachází ve vnějším chování systému. Dalším způsobem modelování, který rozlišujeme, je analogie. Shodu shledáváme v matematické podobnosti fyzikálně odlišných systémů a procesů.[7]

2.1.1 Model procesů pro uvažovaný kyberprostor

Budeme-li vztahovat kyberprostor na počítačový svět, kde se jedná o fyzický svět a svět virtuální, lze sestavit jeho model následujícím způsobem. Startovacím polem uvažujeme hardwarovou základnu se softwarem a různými aplikacemi, která nám vytváří kybernetické služby a data. Toto pole působí na uživatele a naopak, tímto vzniká rozhraní člověk-stroj. Prostředním článkem je všeobecný systém, který se vloží mezi startovací a koncové pole. I v tomto článku je důležité vzájemné působení uživatele a systému. Koncovým polem je již zmíněný fyzický svět. Z tohoto modelu lze usoudit, že kyberprostor obléhá tato jednotlivá pole, tzn. je všude kolem.

2.1.2 Model pro kybernetickou bezpečnost

Při vytváření modelu pro kybernetickou bezpečnost budeme vycházet z modelu pro uvažovaný kyberprostor. Protože kyberprostor je velmi náchylný a lehce napadnutelný například hackery, je nutné v modelu uvažovat o hrozbách, jako jsou válka, špionáže nebo kriminalita. Kybernetickou bezpečností vytvoříme jedno velké pole, které bude podmnožinou kyberprostoru, a zároveň obsáhne pole s již uvedenými hrozbami.

2.1.3 Model pro řešení procesů

Tento model nám bude zobrazovat posloupnost jednotlivých procesů, jejich činnost a to, jaké vstupy a výstupy musí procesy mít, aby správně fungovaly. Model pro řešení procesů bude zobrazován graficky, popřípadě s doplňujícím textem. Cílem vytvoření modelu je většinou všeobecně zvýšit efektivitu a výkonnost zobrazovaných procesů.

Pro vytvoření procesního modelu uspořádáme aktuální informace týkající se fungování společnosti, a to informace o procesech, organizačních strukturách, struktuře produktů a služeb, o strategických cílech ve vazbě na procesy, atd. Nelze sestavit univerzální model. Pro každou organizaci je model jedinečný, protože zobrazuje konkrétní objekty (procesy, činnosti, dokumenty, aplikace) a jejich vazby.

2.2 Možnosti modelování

Při modelování je nutné mít na mysli, že volíme takový nástroj pro modelování, aby se s ním dalo dobře pracovat, a bylo popřípadě možné dělat potřebné úpravy. Použitím modelovacích nástrojů je nám umožněno definování procesu (název, popis, datum, komponenty,…), modelace postupných, souběžných nebo opakujících se průběhů procesů. Dalšími výhodami modelovacích nástrojů jsou grafická zobrazení modelů, podpora pro uchovávání procesů, specifikace úkolů a pracovních kroků. S ohledem na to, že žijeme v „počítačové době“, je tedy na místě využít různé počítačové programy pro modelování procesů.

Počítačové software se zakládají na jednotné databázi a sdílených objektech. Přehledná struktura objektů je uložena v adresářích. Pokud dojde ke změně objektu, dojde k automatické změně všech jeho kopií. Jednou z funkcí je analýza k ověření procesů a k případnému nalezení slabých míst procesů. Po dosažení výsledků se provádí exporty práce do různých formátů. Existuje spousta těchto nástrojů, jejich výčet lze vyhledat na internetu, kde jsou popřípadě i odkazy na konkrétní literaturu zabývající se touto problematikou. Dva známí zástupci těchto softwarových programů jsou ATTIS a ARIS.[34]

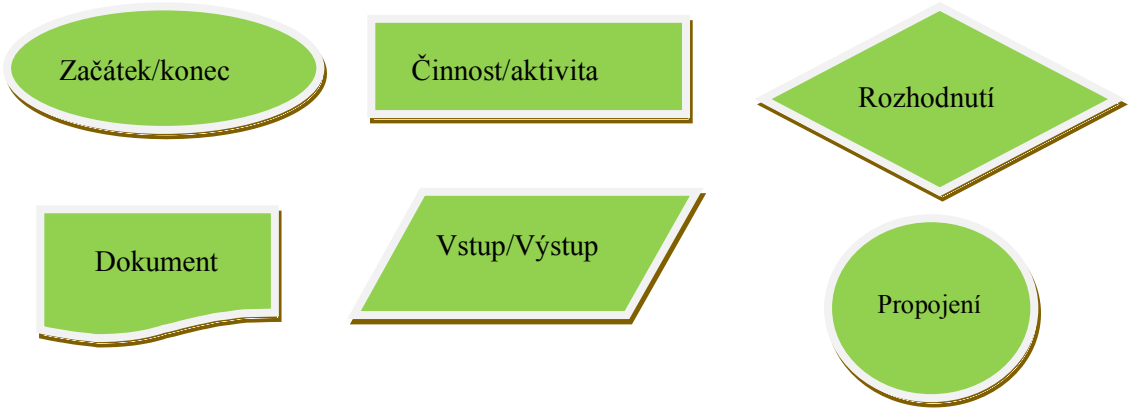
Nástroje pro modelování procesů mohou být:

a) mapa procesů (Process Map)

Mapu procesů nejčastěji používají pro modelování organizace. Jedná se o názorné a přehledné schéma procesů, jejich členění a činnosti. Její koncept lze prezentovat ve dvou úrovních, a to na úrovni univerzální nebo na úrovni detailní. Cílem je usnadnění řízení a rozhodování v dané organizaci. Procesy, které v tomto schématu nalezneme, jsou procesy hlavní, řídící a podpůrné.[21]

b) vývojový diagram (Flow chart)

Velmi používaný a osvědčený nástroj pro modelování procesů. Jde o popis průběhu operací, činností a vztahů mezi nimi, to vše na bázi grafického zobrazení. Vizuální stránka nám tak zajistí průhlednost a jednoduchost procesu. Pro modelování vývojového diagramu jsou popsány základní symboly pomocí geometrických tvarů: začátek/konec, procesní krok(činnost), posloupnost nebo vazba, rozhodování, vstupy/výstupy. Vývojový diagram najde uplatnění zejména v popisu procesu, popisu pracovního postupu, popisu výrobního procesu nebo v popisu algoritmu počítačového programu. Existují různé typy: diagram průběhu prací, vývojový diagram křížového procesu, základní vývojový diagram, diagram IDEFO, diagram SDL, diagram toku dat.[37]



Obr.3. Symboly vývojového diagramu, (Vlastní zpracování)

c) želví diagram (Turtle diagram)

Záměrem toho diagramu je roztřídění klíčových prvků procesu. Ve srovnání s vývojovým diagramem nám jednotlivé prvky nezobrazují symboly geometrických tvarů, ale zobrazení spočívá ve tvaru želvy. Do těla želvy píšeme definici procesu, do hlavy vstup a do ocasu želvy výstup. Otázky typu CO?, KDO?, MĚŘENÍ? a JAK? zapíšeme každou zvlášť do jedné „nohy“.[27]

d) entitně relační diagram

Vychází z metody ERM (Entity-Relationship Model), což je abstraktní a konceptuální znázornění dat. Metoda spočívá ve vytvoření schématu systému a požadavků na tento systém. Schéma a požadavky systému se sestavují od shora dolů.

e) a další …

Jaký postup pro modelování procesu zvolíme, záleží na každém individuálně. Všeobecně bychom měli brát na vědomí následující body. Prvním krokem, který je potřeba udělat, je uvědomit si všechny potřebné procesy, následuje jejich seřazení do logického toku a určení jejich rozsahu. Každý proces má nějaké poslání a cíl, který definujeme. Hlavní činnosti procesu a jejich tok musí být popsán. Po těchto bodech je ještě nutno doplnit odpovědnosti, vstupy a výstupy pro činnosti, zdroje, rizika a přidat textový popis.[32]

2.3 Výzkum pomocí dotazníkového šetření

Pojem výzkum lze definovat jako proces cesty, která má svůj začátek a postupnými kroky se dojde až do samotného cíle. Aby byl proces výzkumu dodržen, je nutné se řídit danými fázemi. Obecně můžeme definovat 4 fáze:

- příprava výzkumu,
- vlastní výzkum,
- zpracování a analýza dat,
- závěr, výzkumná zpráva, prezentace.[10]

Obr.4. Fáze výzkumu (převzato z Petra Fejtková.cz)

Výzkumy se nejčastěji dělí na kvantitativní a kvalitativní. Kvantitativní výzkum spočívá v tom, že si klademe otázky(např. Co? Jak? Kolik?). Postupuje se v něm od něčeho obecného k něčemu konkrétnímu. Založený na testování teorií nebo hypotéz a používají se zde strukturované, standardizované metody. Tento výzkum charakterizuje velký výzkumný vzorek. Výzkum pracuje s čísly a tvrdými daty. Naopak základní otázka u kvalitativního výzkumu je Proč?. Na rozdíl od výzkumu kvantitativního je spíše induktivní, subjektivní a hůře hodnotitelný. Základem je vytváření teorií na bázi rozhovorů nebo pozorování, díky tomu nám stačí menší výzkumný vzorek.

Fáze přípravy výzkumu

První krok, který dá celému výzkumu směr, je výzkumný definování výzkumného problému. Informuje nás o tématu a o tom, jakým způsobem šetření provedeme. Dalším krokem je definování cíle výzkumu. Podle toho, jaký cíl stanovíme, můžeme výzkumy dělit mimo jiné na: orientační, deskriptivní, explanační, prognostické. Jakmile máme stanovený cíl, formulujeme výzkumné otázky, případně hypotézy. Nejčastěji položíme jednu hlavní otázku, dále je možné ji rozdělit na otázky dílčí. Posledním krokem v této fázi je určení metody sběru dat. Mezi ty nejdůležitější a nejvíce používané metody řadíme: pozorování, analýzu dokumentů, dotazování nebo experiment.

Metoda dotazování

Důvodů proč je tato metoda nejpopulárnější je hned několik, například malé náklady, úspora času, anonymita nebo to, že dotazník lze použít opakovaně. Dotazování může být provedeno osobně, telefonicky, poštou nebo on-line, z toho vyplývá, zda bude samotný dotazník ve verzi tištěné nebo on-line.Neopomenutelnou součástí dotazníku musí být průvodní dopis, jehož úkolem je seznámit respondenta s účelem výzkumu, s prohlášením o anonymitě, s osobou provádějící výzkum a v neposlední řadě s tím, jak bude se získanými daty naloženo. Aby byl dotazník úspěšný, musí být otázky správně formulovány. Základní rozdělení otázek je na uzavřené, otevřené, polootevřené. Mezi hlavní vlastnosti otázek řadíme jednoznačnost, jednoduchost, přímost.[38] Pomocí těchto pravidel jsme se i my pokusili sestavit dotazník, kterým budeme zjišťovat mezi občany závislosti související s jejich pohlavím, věkem a kybernetickými útoky na systémy v automobilech. Půjde o dotazník s uzavřenými otázkami, který jsme vytvořili přes aplikaci Google Formuláře.

II. PRAKTICKÁ ČÁST

3 VYHODNOCENÍ KRITÉRIÍ PROCESŮ MODELOVÁNÍM

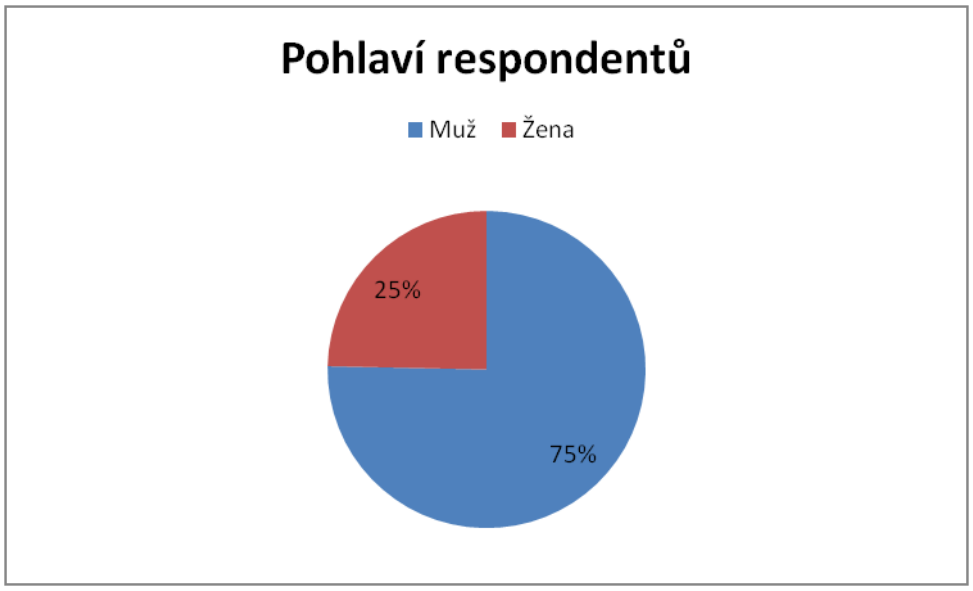
V této kapitole popíšeme výsledky provedeného dotazníkové šetření, jehož účelem bylo prošetřit, jak a zda vůbec lidé vnímají hrozbu kybernetických útoků na automobil. Dalším krokem je vhodné zvolení kritérií procesů a posléze jejich vyhodnocení pomocí vhodně zvolených modelů.

3.1 Dotazníkové šetření

Jednou z metod, kterou jsme se pro tuto práci rozhodli použít, bylo dotazníkové šetření. Pomocí dotazníkového šetření jsme chtěli zjistit, jaký náhled má na tuto problematiku dotazovaná skupina osob. Tyto osoby nebyly předem vybrány. K sestavení dotazníku jsme použili aplikaci od Google, tvorba formulářů. Dotazníkové šetření tedy probíhalo online formou. Dotazník obsahoval 6 uzavřených otázek a jednu otázku s Likertovou škálou. Všechny otázky jsou uvedeny v příloze této práce (příloha PIII). Dotazník byl cílen na respondenty ve věku od 18 let, a zároveň na aktivní řidiče. Respondenti byli oslovováni online formou prostřednictvím sociálních sítí a osobním dotazováním. V rámci dotazníkového šetření byly získány odpovědi od 320 respondentů. Stěžejní otázky pro náš výzkum, ze kterých byla data vyhodnocována, se týkaly pohlaví, věku a hodnocení rizikovosti kybernetického útoku na automobil. Rizikovost byla hodnocena na stupnici 1-5, riziko s číslem 1 bylo definováno jako velmi nízké, riziko číslo 2 jako malé, číslo 3 zastupovalo riziko střední, číslo 4 bylo riziko vysoké a riziko s číslem 5 jsme určili jako velmi vysoké. Data byla vyhodnocena pomocí statistického programu IBM SPSS(verze 23), pro statistické testování byl použit G-test nezávislosti, vzhledem k charakteru sesbíraných dat, která vykazují menší hodnoty očekávaných četností, než jaké by bylo potřeba. Pro srovnání testování dle G-testů jsou uvedeny i hodnoty vycházející z Pearsonova chí-kvadrát testu nezávislosti.

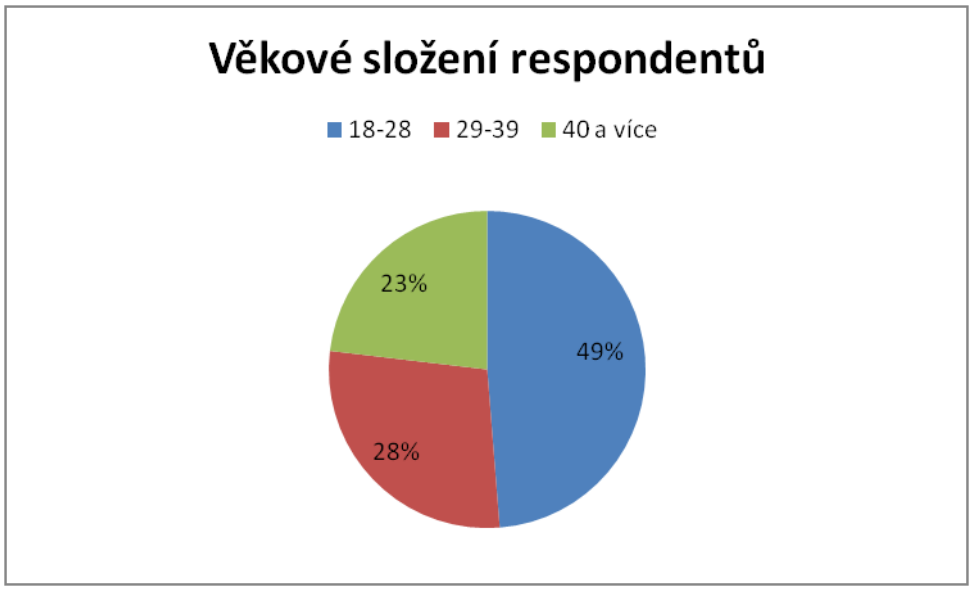
3.1.1 Dosažené výsledky

V této podkapitole jsme uvedli vyhodnocení dotazníkového šetření, jehož cílem bylo zjistit povědomí lidí o kybernetických útocích na automobil. Ze získaných dat jsme vytvořili vypovídající grafy a pomocí statistického testování v programu zjistili závislosti mezi pohlavím, věkem respondentů a jejich hodnocením rizikovosti kybernetického útoku na automobil.



Obr.5. Graf zastoupení pohlaví respondentů (Vlastní zpracování)

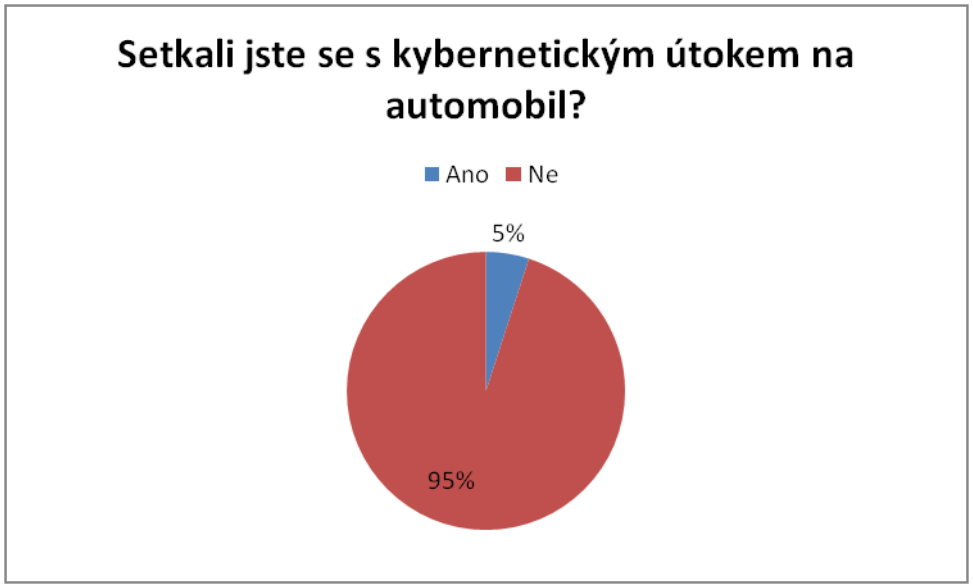
Na obrázku (Obr.5) lze vidět, že z celkového počtu 320 respondentů, dotazník vyplnilo pouhých 25% osob ženského pohlaví. Naopak dotazník vyplanilo 75% mužů. Tento výsledek může, být ovlivněn tématem dotazníkového šetření. Ženy se všeobecně méně zajímají o věci spojené s automobilovou tématikou.



Obr.6. Graf věkového složení respondentů (Vlastní zpracování)

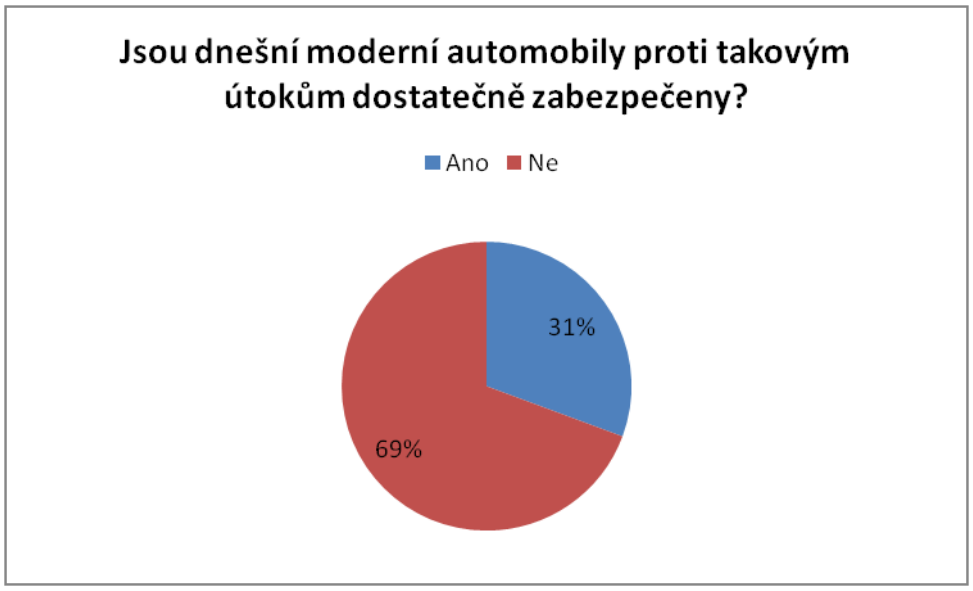
Z obrázku (Obr.6) je zřejmé, že co se týče věkového složení, je zde nejvíce zastoupena skupina respondentů ve věku od 18 – 28let, která tvoří téměř dvě třetiny respondentů, a to

49%. Zbylé dvě věkové kategorie 29 – 39 let a 40 a více let jsou zastoupeny téměř stejným procentuální podílem.



Obr.7. Graf povědomí o kybernetickém útoku na automobil (Vlastní zpracování)

Obrázek (Obr.7) zobrazuje odpovědi na otázku, jestli se respondenti setkali s kybernetickým útokem na automobil. Z odpovědí je vidět, že celých 95% respondentů se s tímto typem útoku doposud nesetkalo. Malé procento kladných odpovědí respondentů nám značí, že se tyto útoky reálně vyskytují.



Obr.8. Graf vyhodnocení názorů respondentů ohledně zabezpečení automobilů

(Vlastní zpracování)

Na obrázku (Obr.8) vidíme názor respondentů na to, jestli jsou podle nich dnešní moderní automobily dostatečně zabezpečeny. Téměř 70 % respondentů se neztotožňuje s tím, že by automobily byly dostatečně zabezpečeny. Ovšem 31% respondentů si myslí, že zabezpečení vozů je dostatečné.

Statistické testování

Cíl výzkumu:

Cílem dotazníkového šetření bylo prozkoumat povědomí občanů České republiky o kybernetických útocích na automobil a o rizicích s nimi spojenými.

Výzkumné otázky:

Aby se podařilo naplnit cíl výzkumu, určili jsme čtyři výzkumné otázky. Na základě těchto otázek byly poté stanoveny výzkumné hypotézy.

- Výzkumná otázka č.1: Existuje závislost mezi pohlavím a vnímanou rizikovostí kybernetických útoků na multimediální systém v automobilu?
- Výzkumná otázka č.2: Existuje závislost mezi pohlavím a vnímanou rizikovostí kybernetických útoků na systém zamykání a odemykání automobilu?

- Výzkumná otázkač.3: Existuje závislost mezi věkem a vnímanou rizikovostí kybernetických útoků na multimediální systém v automobilu?
- Výzkumná otázka č.4: Existuje závislost mezi věkem a vnímanou rizikovostí kybernetických útoků na systém zamykání a odemykání automobilu?

Statistické hypotézy:

Pro každou výzkumnou otázku byly stanoveny dvě statistické hypotézy. Statistická hypotéza H_0 jako nulová hypotéza a H_1 jako hypotéza alternativní. Za proměnné jsme v prvních dvou otázkách zvolili *pohlaví* a *rizikovost* a ve zbylých dvou otázkách *věk* a *rizikovost*.

Testování nezávislosti mezi rizikovostí a pohlavím

Statistické hypotézy pro výzkumnou otázku č.1

H_0: Neexistuje statisticky významná závislost mezi pohlavím a vnímanou rizikovostí kybernetických útoků na multimediální systém v automobilu.

H_1: Existuje statisticky významná závislost mezi pohlavím a vnímanou rizikovostí kybernetických útoků na multimediální systém v automobilu.

Výsledky testování:

Tab.1. Test závislosti rizikovosti na pohlaví při kybernetickém útoku na multimediální systém v automobilu (Vlastní zpracování)

			Rizikovost - Kybernetický útok na multimediální systém					Celkem
			1	2	3	4	5	
Pohlaví	Muž	Pozorovaná četnost	8	40	74	102	10	234
		Očekávaná četnost	5,9	35,1	70,2	111,2	11,7	234,0
		Relativní hodnota četnosti	3,4%	17,1%	31,6%	43,6%	4,3%	100,0%
		Reziduum	2,2	4,9	3,8	-9,1	-1,7	
	Žena	Pozorovaná četnost	0	8	22	50	6	86
		Očekávaná četnost	2,2	12,9	25,8	40,9	4,3	86,0
		Relativní hodnota četnosti	0,0%	9,3%	25,6%	58,1%	7,0%	100,0%
		Reziduum	-2,2	-4,9	-3,8	9,2	1,7	
Celkem		Pozorovaná četnost	8	48	96	152	16	320
		Očekávaná četnost	8,0	48,0	96,0	152,0	16,0	320,0
		Relativní hodnota četnosti	2,5%	15,0%	30,0%	47,5%	5,0%	100,0%

Pro účely statistického testování nulové hypotézy byla stanovena hladina významnosti $\alpha=0,05$.

Z tabulky (Tab.1) je zřejmé, že u mužů je reziduum vyšší u rizika 1, 2 a 3, naopak u rizika 4 a 5 nabývá záporných hodnot. To znamená, že muži tomuto útoku přikládají menší riziko(1,2,3) a oproti tomu ženy, mají reziduum celkem vysoké u rizika 4 arizika 5, které se pohybuje nad nulou. Můžeme říct, že tento útok ženy vnímají jako rizikovější.

Tab.2. Chí - kvadrát test (Vlastní zpracování)

	Hodnota testu	p-hodnota
Pearsonův chí-kvadrát test	9,973[a]	,041
G-test	12,153	,016

Na základě provedeného testu byla zjištěna p-hodnota = 0,016, takže test zamítá na pětiprocentní hladině významnosti hypotézu H_0 o nezávislosti. S pětiprocentním rizikem omylu můžeme tedy říci, že vnímaná rizikovost kybernetického útoku na multimediální systém závisí na pohlaví.

Statistické hypotézy pro výzkumnou otázku č.2

H_0: Neexistuje statisticky významná závislost mezi pohlavím a vnímanou rizikovostí kybernetických útoků na systém zamykání a odemykání automobilu.

H_1: Existuje statisticky významná závislost mezi pohlavím a vnímanou rizikovostí kybernetických útoků na systém zamykání a odemykání automobilu.

Výsledky testování:

Tab.3. Test závislosti rizikovosti na pohlaví při kybernetickém útoku na systém zamykání a odemykání automobilu (Vlastní zpracování)

			Rizikovost - Kybernetický útok na systém zamykání a odemykání					Celkem
			1	2	3	4	5	
Pohlaví	Muž	Pozorovaná četnost	90	52	60	8	24	234
		Očekávaná četnost	83,4	52,7	60,0	11,7	26,3	234,0
		Relativní hodnota četnosti	38,5%	22,2%	25,6%	3,4%	10,3%	100,0%
		Reziduum	6,6	-,6	,0	-3,7	-2,3	
	Žena	Pozorovaná četnost	24	20	22	8	12	86
		Očekávaná četnost	30,6	19,4	22,0	4,3	9,7	86,0
		Relativní hodnota četnosti	27,9%	23,3%	25,6%	9,3%	14,0%	100,0%
		Reziduum	-6,6	,7	,0	3,7	2,3	
Celkem		Pozorovaná četnost	114	72	82	16	36	320
		Očekávaná četnost	114,0	72,0	82,0	16,0	36,0	320,0
		Relativní hodnota četnosti	35,6%	22,5%	25,6%	5,0%	11,3%	100,0%

Pro účely statistického testování nulové hypotézy byla stanovena hladina významnosti α=0,05.

Z tabulky (Tab.3) vyplynulo, že muži mají reziduum vyšší pouze u rizika 1, rizika 2, 3, 4 a 5 nabývají záporných hodnot, tudíž jim nepřikládají téměř žádnou váhu. Reziduum u žen nabývá vyšších hodnot u rizika 4 a 5. Muži tomuto útoku přikládají mnohem menší rizikovost než ženy. Můžeme říct, že tento útok ženy vnímají jako rizikovější.

Tab.4.Chí – kvadrát test (Vlastní zpracování)

	Hodnota testu	p-hodnota
Pearsonův chí-kvadrát test	7,114[a]	,130
G-test	6,681	,154

Na základě provedeného testu byla zjištěna p-hodnota = 0,154, takže test nezamítá na pěti-procentní hladině významnosti hypotézu H_0 o nezávislosti.

S pětiprocentním rizikem omylu můžeme tedy říci, že vnímaná rizikovost kybernetického útoku na systém zamykání a odemykání nezávisí na pohlaví.

Testování nezávislosti mezi rizikovostí a věkem

Statistické hypotézy pro výzkumnou otázku č.3

H_0: Neexistuje statisticky významná závislost mezi věkem a vnímanou rizikovostí kybernetických útoků na multimediální systém v automobilu.

H_1: Existuje statisticky významná závislost mezi věkem a vnímanou rizikovostí kybernetických útoků na multimediální systém v automobilu.

Výsledky statistického testování:

Tab.5. Test závislosti rizikovosti na věku při kybernetickém útoku na multimediální systém v automobilu (Vlastní zpracování)

			Rizikovost - Kybernetický útok na multimediální systém					Celkem
			1	2	3	4	5	
Věk	18-28	Pozorovaná četnost	6	22	46	76	6	156
		Očekávaná četnost	3,9	23,4	46,8	74,1	7,8	156,0
		Relativní hodnota četnosti	3,8%	14,1%	29,5%	48,7%	3,8%	100,0%
		Reziduum	2,1	-1,4	-,8	1,9	-1,8	
	29-39	Pozorovaná četnost	2	14	26	44	4	90
		Očekávaná četnost	2,3	13,5	27,0	42,8	4,5	90,0
		Relativní hodnota četnosti	2,2%	15,6%	28,9%	48,9%	4,4%	100,0%
		Reziduum	-,3	,5	-1,0	1,3	-,5	
	40 a více	Pozorovaná četnost	0	12	24	32	6	74
		Očekávaná četnost	1,9	11,1	22,2	35,2	3,7	74,0
		Relativní hodnota četnosti	0,0%	16,2%	32,4%	43,2%	8,1%	100,0%
		Reziduum	-1,9	,9	1,8	-3,2	2,3	
Celkem		Pozorovaná četnost	8	48	96	152	16	320
		Očekávaná četnost	8,0	48,0	96,0	152,0	16,0	320,0
		Relativní hodnota četnosti	2,5%	15,0%	30,0%	47,5%	5,0%	100,0%

Pro účely statistického testování nulové hypotézy byla stanovena hladina významnosti α=0,05.

Z tabulky (Tab.5) můžeme vyčíst, že věková skupina 18 – 28let má reziduum vyšší u rizika 1 a 4, zbylá rizika 2, 3, 5 nabývají záporných hodnot.

Věková skupina 29 – 39let má reziduum ve všech rizicích pohybující se kolem nuly. Podobné hodnoty rezidua jako u první věkové skupiny, nabývají i hodnoty rezidua u věkové skupiny 40 a více let, liší se však v rizicích. Tato skupina má s vyšším reziduem rizika 3 a 5.Nelze tedy úplně přesně říct, která věková skupina tento útok vnímá jako rizikovější.

Tab.6. Chí – kvadrát test (Vlastní zpracování)

	Hodnota testu	p-hodnota
Pearsonův chí-kvadrát test	5,649[a]	,687
G-test	7,153	,520

Na základě provedeného testu byla zjištěna p-hodnota = 0,520, takže test nezamítá na pěti-procentní hladině významnosti hypotézu H_0 o nezávislosti. S procentním rizikem omylu můžeme tedy říci, že vnímaná rizikovost kybernetického útoku na multimediální systém nezávisí na věku.

Statistické hypotézy pro výzkumnou otázku č.4

H_0: Neexistuje statisticky významná závislost mezi věkem a vnímanou rizikovostí kybernetických útoků na systém zamykání a odemykání automobilu.

H_1: Existuje statisticky významná závislost mezi věkem a vnímanou rizikovostí kybernetických útoků na systém zamykání a odemykání automobilu.

Tab.7. Test závislosti rizikovosti na věku při kybernetickém útoku na multimediální systém v automobilu (Vlastní zpracování)

			Rizikovost - Kybernetický útok na systém zamykání a odemykání					Celkem
			1	2	3	4	5	
Věk	18-28	Pozorovaná četnost	52	30	46	14	14	156
		Očekávaná četnost	55,6	35,1	40,0	7,8	17,6	156,0
		Relativní hodnota četnosti	33,3%	19,2%	29,5%	9,0%	9,0%	100,0%
		Reziduum	-3,6	-5,1	6,0	6,2	-3,6	
	29-39	Pozorovaná četnost	28	32	18	2	10	90
		Očekávaná četnost	32,1	20,3	23,1	4,5	10,1	90,0
		Relativní hodnota četnosti	31,1%	35,6%	20,0%	2,2%	11,1%	100,0%
		Reziduum	-4,1	11,8	-5,1	-2,5	-,1	
	40 a více	Pozorovaná četnost	34	10	18	0	12	74
		Očekávaná četnost	26,4	16,7	19,0	3,7	8,3	74,0
		Relativní hodnota četnosti	45,9%	13,5%	24,3%	0,0%	16,2%	100,0%
		Reziduum	7,6	-6,7	-1,0	-3,7	3,7	
Celkem		Pozorovaná četnost	114	72	82	16	36	320
		Očekávaná četnost	114,0	72,0	82,0	16,0	36,0	320,0
		Relativní hodnota četnosti	35,6%	22,5%	25,6%	5,0%	11,3%	100,0%

Pro účely statistického testování nulové hypotézy byla stanovena hladina významnosti α=0,05.

Z tabulky (Tab.7) vyplývá, že věková skupina 18 – 28let má nejvyšší reziduum u rizika 3 a 4, zbylá rizika 2, 3, 5 nabývají záporných hodnot. Věková skupina 29 – 39let má nejvyšší reziduum u rizika 2. Hodnoty rezidua u věkové skupiny 40 a více let, jsou nejvyšší u rizika 1 a 5. Je tedy zřejmé, že každá věková skupina tento útok vnímá jinak rizikový.

Tab.8. Chí – kvadrát test (Vlastní zpracování)

	Hodnota testu	p-hodnota
Pearsonův chí-kvadrát test	27,600[a]	,001
G-test	29,919	,000

Na základě provedeného testu byla zjištěna p-hodnota = 0,000, takže test zamítá na pěti-procentní hladině významnosti hypotézu H_0 o nezávislosti. S pětiprocentním rizikem omy-

lu můžeme tedy říci, že vnímaná rizikovost kybernetického útoku na systém zamykání a odemykání závisí na věku.

3.2 Volba kritérií procesu a jejich hodnocení

Abychom mohli namodelovat procesy, bylo vhodné zvolit si kritéria. Uvažovali jsme taková kritéria, která mohou ovlivňovat napadení automobilu. Prvním kritériem je *stáří automobilu*, dalším *čas potřebný k napadení vozidla* a posledním kritérium jsme zvolili *technické vybavení potřebné k napadení automobilu.*

Stáří automobilu je důležitým kritériem, protože technologický vývoj jde mílovými kroky kupředu. V obou dále modelovaných procesech toto kritérium hraje velkou roli. Dalo by se říct, že čím novější automobil, tím je z hlediska kybernetických útoků snadnější cíl. V této práci uvažujeme ty modernější automobily, které mají multimediální rozhraní.

3.2.1 Stáří automobilu

Napadení systémů:

První klasické palubní počítače se do automobilů začaly zavádět již v 80.letech, samozřejmě jejich postupný vývoj vedl k neustálému zlepšování.[2[22]2] Kolem roku 2001 se tyto palubní počítače začaly rozšiřovat o nová multimediální rozhraní. V posledních pěti letech dosahují multimediální systémy v automobilech velmi vysoké úrovně. [23];[18]

Zamykání a odemykání:

Stejně tak jako u napadení systému, kdy se objevují první palubní počítače se v 80.letech objevují první známky vzdáleného systému bez klíče. [29] Vynález pasivního systému pro bezklíčový vstup se datuje do let devadesátých. V roce 2015 jsme se již mohli setkat s otevíráním automobilu, které spočívalo pouze v dotyku na určité místo na karoserii.[30] Největší novinka je od roku 2017 odemykání a zamykání automobilu pomocí aplikace v telefonu.[36]

3.2.2 Čas potřebný k napadení vozidla:

Napadení systémů a zamykání a odemykání:

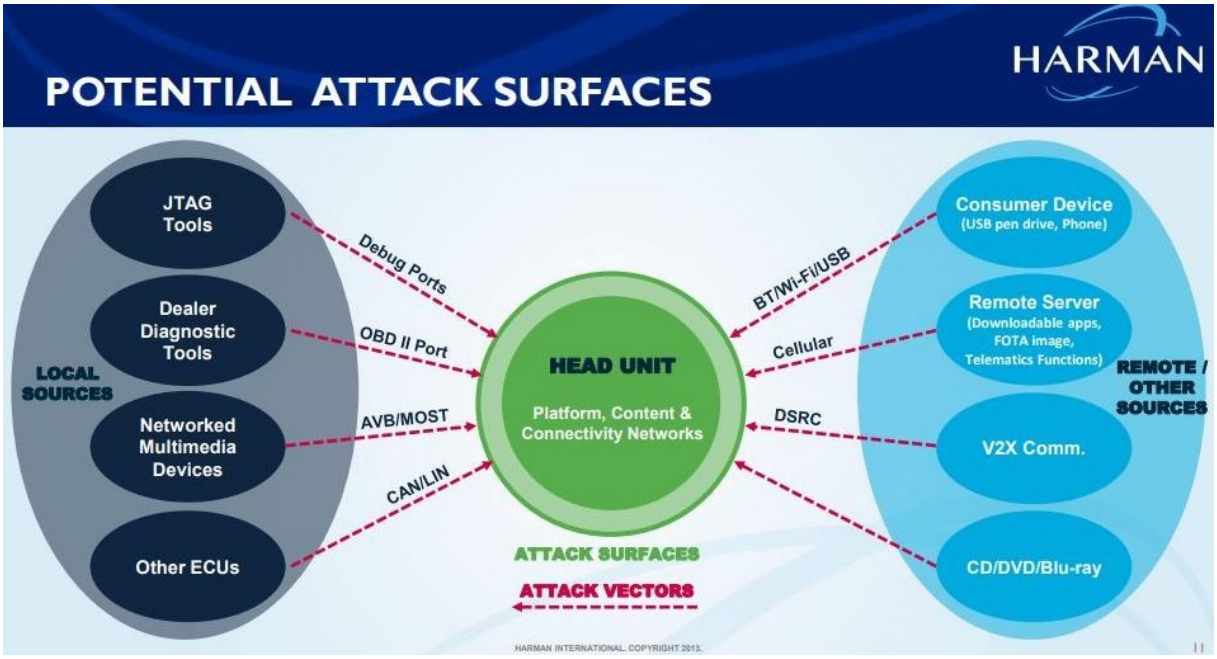
Čas je v tomto ohledu významnou proměnnou, odvíjí se samozřejmě od spousty faktorů. Podle různých zdrojů se uvádí, že čas potřebný k napadení automobilu

kybernetickým útokem na multimediální systém a systém zamykání a odemykání je v rozmezí jen několika pár minut, což záleží samozřejmě na zkušenostech útočníka a také na technickém vybavení.

3.2.3 Technické vybavení potřebné k napadení vozidla:

Napadení systémů:

Z obrázku (Obr.9) můžeme vyčíst, že jsou dvě potenciální strany, ze kterých může být kybernetický útok na automobil realizován. Strana nazvaná jako Local Sources (místní zdroje) vybízí k útokům prostřednictvím JTAG Tools pomocí ladění portů, diagnostických zařízení (OBD II porty), síťových multimediálních zařízení pomocí systémů AVB(Audio Video Bridging) nebo MOST(Media Oriented System Transport), samozřejmě nesmíme opomenout řídící jednotky. Kybernetické útoky ze strany Remote/Other Sources(vzdálené zdroje) je možné realizovat díky spotřebnímu zařízení, jehož příkladem může v automobilu být USB či telefon, vzdáleným serverům, které reprezentují stahování aplikací nebo telematické funkce. Dále také V2X Comm. či CD/DVD.[1] Ať už kybernetický útok přichází z kterékoli strany, napadá hlavní jednotku.



Obr.9. Potential attack surfaces (převzato z GENIVI Open Source Projects Wiki, 2016, s.11)

Má-li automobil byť jen jedinou s těchto uváděných komponent, pak stačí útočníkovi už jen například obyčejný chytrý telefon a notebook či tablet k provedení kybernetického útoku.

Zamykání a odemykání

U systému zamykání a odemykání automobilu je princip velmi jednoduchý, k tomu, aby byl kybernetický útok realizován, postačí útočníkovi pouze dobře sestrojený zesilovač radiových vln.[3]

3.3 Vyhodnocení kritérií procesu

Na obrázku č. 6 je vyjádřen zjednodušený modelovaný proces napadení systému zamykání a odemykání automobilu.Model jsme vytvářeli v programu PowerDesigner. Na modelu můžeme vidět, že pro „zkušeného útočníka“, který má potřebné vybavení, může být velmi snadné automobil napadnout a dále s ním manipulovat.

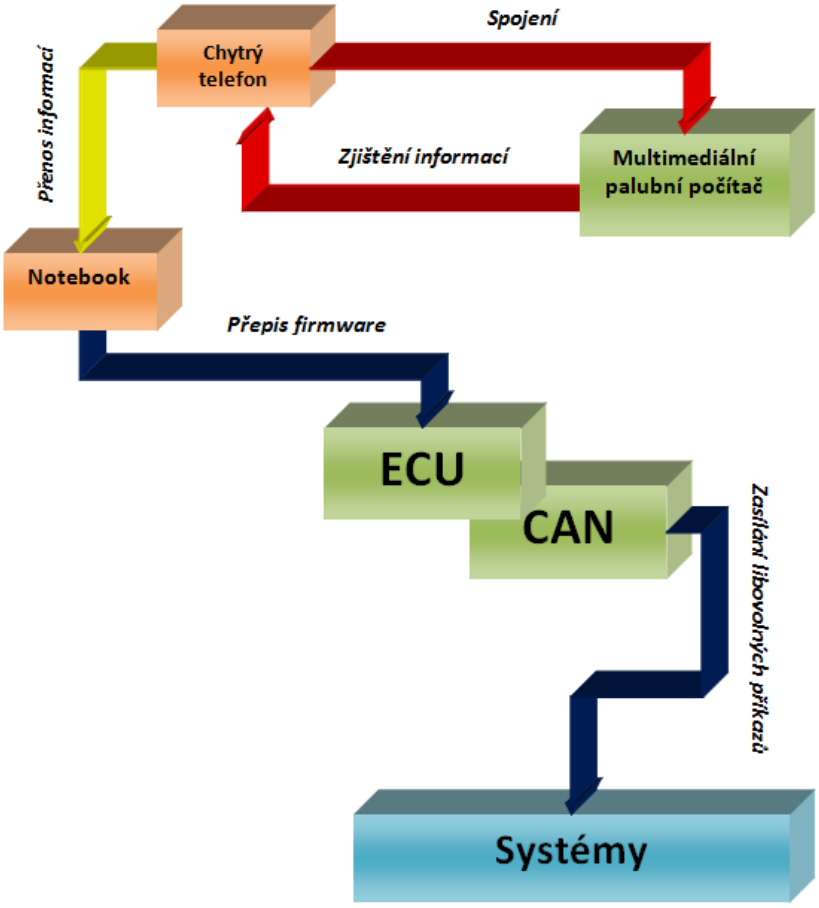
Na modelu jsou zobrazeny dva toky procesů. Jeden tok procesu je ze strany uživatele automobilu a druhý tok procesu ze strany útočníka. Procesy probíhají následovně. Na modelu je zřejmé, že v prvním kroku nám nastávají dva souběžné procesy. Těmi jsou stisk tlačítka na dálkovém ovládání uživatelem a aktivace přenosného zařízení útočníkem.V návaznosti na předešlé procesy následují další dva procesy probíhající souběžně. Proces na straně uživatele probíhá tak, že dálkové ovládání vysílá bezpečnostní kód. Proces na straně útočníka spočívá v načtení signálu vyslaného kódu a následném dekódování jeho frekvence. Na modelu můžeme vidět, že v tomto kroku dochází k celkem třem současně běžícím procesům. Dále se nám zobrazují opět dva procesy, které by se daly považovat souběžné. Když dochází k samotnému uzamčení automobilu na straně uživatele, útočník úspěšně odhaluje onen bezpečnostní kód. V posledním kroku toho kybernetického útoku na systém zamykání a odemykání dochází k momentu, kdy uživatel odchází od automobilu a útočník využívá situace k odemčení automobilu a následné manipulaci s ním. Útočník má možnost v tomto okamžiku automobil ukrást a odjet s ním nebo pokračovat v dalším kybernetickém útoku na multimediální systém.

Obr.10. Proces napadení kybernetického systému zamykání a odemykání vozidla, (Vlastní zpracování)

Tento proces byl v praxi testován německým autoklubem ADAC. Poprvé jej autoklub testoval v roce 2016 a podruhé tento test zopakoval v roce 2017, v tomto případě ovšem ne moc úspěšně. Kontrolní test spočíval v použití jednoduchého zesilovače a probíhal obdobně jako proces zobrazený v obrázku výše (Obr.6). Automobily, na kterých byl test prováděn, byly většinou vyrobeny mezi lety 2015-2017. Tato informace, ale neznamená, že se test modelů týkal pouze tohoto automobilů vyrobených v tomto rozmezí. Testované modely byly i mnohem staršího data výroby. Mezi snadno napadnutelné vozy patří i vozy značky Škoda, Peugeot nebo Tesla. V příloze (příloha PII) práce je uvedena tabulka, ve které nalezneme detailní přehled testovaných automobilů.[5]

Na obrázku (Obr.11) je namodelovaný proces kybernetického útoku na multimediální systém v automobilu. Je nutné zmínit, že možností napadení těchto systému je více. Přes multimediální systém v automobilu může útočník napadnout například brzdový systém, systém hlídání tlaku v pneumatikách, systém řízení nebo třeba systém GPS. Jelikož jsou v nových automobilech dnes již zcela běžně umísťovány multimediální palubní počítače, které mimo jiné umožňujii připojení k internetu a tím propojení s mobilním telefonem, riziko napadení útočníkem se zvětšuje. Pro zkušeného útočníka s příslušným technickým vybavenímje velmi jednoduché se s tímto palubním počítačem spojit. Útočník získá potřebné informace,

které přenese například jako model do svého notebooku, případně jiného kompetentního zařízení. Vzhledem k jeho přepokládaným zkušenostem není problém vygenerovat kybernetický útok tak, aby se v řídící jednotce a kyberprostoru automobilu začal přepisovat vhodný proces ve škodlivý firmware. Prostřednictvím škodlivého firmware a ve spolupráci řídící jednotky se sběrnicí CAN se vygeneruje příkaz, který zadal útočník. A poté jsou útočníkem vysílány další potřebné příkazy k ovládnutí již uvedených systémů.



Obr.11. Proces napadení automobilu přes multimediální systém (Vlastní zpracování)

Proces byl namodelován i na základě experimentu, který v praxi provedli dva výzkumníci Charlie Miller a Chris Valasek. Celý tento experiment, byl v roce 2015 jedním z největších spouštěčů řešení problematiky kybernetických útoků na automobily. Charlie Miller a Chris Valasek využili ke svému pokusu automobil Jeep Cherokee. Tento vůz má ve své výbavě palubní multimediální systém Uconnect a umožňuje tím pádem internetové připojení ve vozidle, což je pro kybernetický útok na automobil stěžejní vlastnost. Díky internetovému připojení mohli prostřednictvím telefonu zjistit potřebné informace (především se jednalo o

IP adresy). Dále jim stačilo, aby si pořídili modem příslušného telefonního operátora a dosáhli tak stejných IP rozsahů. Poté už těmto výzkumníkům stačilo jen se pohodlně usadit s notebookem doma na pohovce a pomocí zjištěných informací a potřebného technologického vybavení, provést na dálku útok na příslušný prvek ve vozidle. V tomto případě útočili na chip, který komunikuje se sběrnicemi CAN. Pozměněním firmware v chipu došlo k restartu celého palubního multimediálního systému. Po restartu už mohli výzkumníci zasílat pokyny na CAN sběrnice a tím ovládat celý automobil. [13];[42]

4 NÁVRH PROCESŮ Z HLEDISKA KYBERNETICKÉ BEZPEČNOSTI

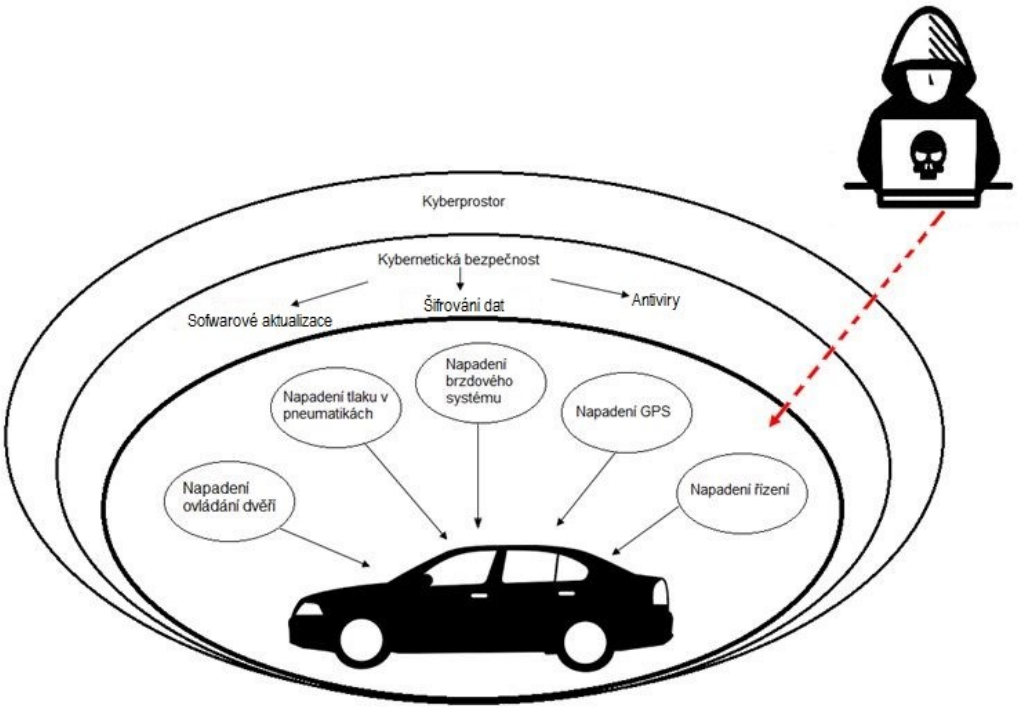
Namodelované procesy jsou z hlediska kybernetické bezpečnosti velmi málo ošetřené. Proto je potřebné teoreticky navrhnout, jakým způsobem by se daly tyto procesy zabezpečit, tak aby bylo riziko kybernetického útoku co nejmenší nebo nejlépe vůbec žádné. A právě tomu se budeme věnovat v následující kapitole.

4.1 Návrh řešení pro model procesu kybernetického útoku na systém zamykání a odemykání automobilu

Návrhy na řešení kybernetické bezpečnosti u procesu kybernetického útoku na systém zamykání a odemykání automobilu spočívají hlavně v mechanických zabezpečeních. To protože tento proces útoku, popsaný v kapitole 3.3.1, je otázkou spíše mechanickou. Doporučení jak automobil zabezpečit, je například použít na dálkové ovládání kapsičky či obaly, které mají stínící funkci, a tím pádem blokují signál, které ovládání vysílá.[12] Dále by uživatel automobilu měl dálkové ovládání nechávat uložené v co největší vzdálenosti od automobilu tak, aby signál byl co nejslabší.[15] Nejnovějším systémem, který by měl být schopný ochránit automobil, je systém VAM. Funguje na bázi elektromechanického zabezpečení a podle průzkumů jej útočníci doposud nezdolali. Jeho nespornou výhodou je totiž to, že je pro každé vozidlo individuální a používá ojedinělý logický kód.[40]

4.2 Návrh řešení pro model procesu kybernetického útoku na systémy v automobilu

Pro pochopení modelu procesu kybernetického útoku na systémy v automobilu z hlediska kybernetické bezpečnosti jsme vytvořili následující model, který zobrazuje celkové pojetí popisované problematiky na obrázku (Obr.12). Primárním prvkem tohoto modelu je automobil, který se stane cílem kybernetického útoku. Předpokládáme, že tento automobil je vybaven právě multimediálním systémem. Tento systém zahrnuje jednotlivé podsystémy: ovládání dveří, hlídání tlaku v pneumatikách, brzd, GPS či řízení, atd. Aby se útočník mohl dostat do tohoto multimediálního systému, musí vniknout do kyberprostoru automobilu a překonat námi navrženou sféru kybernetické bezpečnosti automobilu. Do této sféry řadíme například softwarové aktualizace, šifrování dat a antiviry.



Obr.12.Systémové pojetí problematiky kybernetického útoku na systémy v automobilu, (Vlastní zpracování)

Antiviry

V roce 2015 přišla izraelská firma TowerSec s programem ECUShield, který by měl fungovat obdobně jako klasické počítačové antiviry. Má za cíl chránit právě výše zmíněné systémy v obrázku(Obr.8) a to tak, že zablokuje jakýkoli pokus okybernetický útok na automobil jak zvenčí, tak i zevnitř.[2] ECUShield se snadno integruje do řídící jednotky se sběrnicí dat CAN-BUS, telematického ovladače nebo informačního zařízení, tímto se z něj stává systém detekce a prevence narušení a proto může nepřetržitě sledovat vozidlo a případně identifikovat nové hrozby.[9]

Šifrování dat

K šifrování dat jsou vyvinuty speciální programy, které posílají zašifrovaná data na vzdálený server. Díky těmto programům by také mohl uživatel automobilu rozhodovat o sdílení dat o vozidle například s výrobcem, servisem či pojišťovnou.[20] Další možností, kterou lze považovat za kybernetické zabezpečení, je šifrování založené na certifikátech například HTTPS. Pak útočníkovi nepomůže ani to, že zná šifrovací klíč.[16]

Pravidelné softwarové aktualizace

U toho typu zabezpečení museli uživatelé automobilů často do servisu, kde jim příslušný software zaktualizovali. Což spousta uživatelů nevyužívala. Letos ovšem přišla společnost Continental s inovativním řešením zabezpečení. Vymysleli způsob, jak bude možné provádět aktualizace softwarů v multimediálním systému na dálku pomocí mobilních telefonů. V okamžiku, kdy vyjde nová aktualizace, budou díky tomuto řešení vozidla ihned zabezpečenana tu doposud nejvyšší bezpečnostní úroveň. [19]

ZÁVĚR

Tato bakalářská práce popisovala problematiku užití procesního inženýrství v kybernetické bezpečnosti. Na začátku práce jsme definovali základní pojmy a koncepty potřebné k uvedení do tématu práce. Poté jsme se pokusili aplikovat vybrané a definované pojmy procesního inženýrství v kybernetické bezpečnosti na konkrétní model. Pro vytvoření modelu jsme zvolili jeden konkrétní příklad a to kybernetický útok na osobní automobil a jeho systémy. I zde jsme se ale snažili tento příklad co nejvíce konkretizovat, jelikož ze studia literatury, zahraničních studií a reálných příkladů vyplynulo, že způsobů napadení může být celá řada. Vybrali jsme si pouze dva případy, které jsme v praktické části zpracovávali - kybernetický útok na systém zamykání a odemykání automobilu a kybernetický útok na multimediální systémy v automobilu.

Dříve, než jsme přikročili k samotnému vyhodnocení kritérií procesu, rozhodli jsme se pro dotazníkové šetření. Hlavním cílem bylo zjistit, jak lidé přistupují k problematice kybernetické bezpečnosti a zda si hrozby s kybernetickými útoky vůbec uvědomují. Zaměřili jsme se přitom na spojitost pohlaví dotazovaných, jejich věk a jejich názor na kybernetický útok na systémy v automobilu. Výzkumná otázka č. 1 se ptala na existenci závislosti mezi pohlavím dotazovaného a rizikovostí kybernetických útoků na multimediální systém v automobilu. Dalo by se totiž předpokládat, že hodnotí-li tuto problematiku muži nebo ženy v různém věkovém rozmezí, můžou se jejich názory lišit. Výsledek testování byl, že je zde jistá možnost této závislosti. Muži si více připouští riziko toho typu napadení automobilu. Druhá výzkumná otázka zjišťovala, zda existuje závislost mezi pohlavím a vnímanou rizikovostí kybernetických útoků na systém zamykání a odemykání automobilu. V tomto případě bylo šetřením zjištěno, že s určeným rizikem omylu zde závislost není. Úkolem třetí výzkumné otázky bylo zjistit, jestli existuje závislost mezi věkem a vnímanou rizikovostí kybernetických útoků na multimediální systém v automobilu. Zde můžeme opět s jistým rizikem závislost vyloučit. A čtvrtá výzkumná otázka zjišťovala závislost mezi věkem a vnímanou rizikovostí kybernetických útoků na systém zamykání a odemykání automobilu. V tomto případě byla závislost s jistou možností omylu potvrzena Některé hypotézy se nám potvrdily a některé ne. Dotazník tedy posloužil k drobnému přehledu o povědomí běžných uživatelů automobilů o možnostech kybernetických útoků. Nešlo o žádný zásadní výzkum, sloužil pouze jako opora pro výzkumníky při tvorbě této práce.

Dále jsme se zaměřili už na samotné zvolené procesy, kterými byly - kybernetický útok na systém zamykání a odemykání automobilu a kybernetický útok na multimediální systém v automobilu. Nejdříve jsme zvolili několik kritérií, které by mohly procesy ovlivnit. Byly jimi například stáří automobilu, čas potřebný k ukradení vozidla a technické vybavení potřebné k napadení automobilu. Tato kritéria jsme následně vyhodnotili a začlenili je do modelů procesů. Oba procesy byly namodelovány a popsány za účelem lepšího pochopení popisované problematiky. Pokud bychom měli krátce shrnout průběh těchto procesů, v prvním případě by kybernetický útok na zamykání a odemykání vozidla začal ze strany útočníka aktivací potřebného zařízení k zachycení signálu z dálkového ovládání, pak následuje příjem a dekódování signálu a skončil by odemčením vozidla a s největší pravděpodobností jeho krádeží. Druhý námi vytvořený model popisuje kybernetický útok na multimediální systém. Takovýto útok by mohl začít tak, že útočník by se do multimediálního systému dostal pomocí chytrého telefonu, díky internetovému připojení toho systému. Získá-li útočník potřebné informace dojde k napojení na řídící jednotky jednotlivých systémů a jejich ovládnutí. Uživatel vozidla je při takovém napadení bezmocný, takže může jen čekat, co útočník provede, ať už s řízením nebo například s brzdami. Trochu odlišné je v tomto napadení systémů GPS, kdy zároveň dochází ke ztrátě uživatelovi osobní identity. V obou případech může dojít k ohrožení osoby na životě. Tyto typy kybernetických útoků se mohou různě lišit, ať už v jejich provedení nebo svými následky. Uvedené typy útoků jsou pouze modelovými příklady.

V poslední části práce jsme se pokusili vytvořit návrh řešení procesů z hlediska kybernetické bezpečnosti. Pro každý proces jsme navrhli způsob zabezpečení tak, aby se dalo útokům předejít nebo je přinejmenším znesnadnit. U procesu, který se týkal kybernetického útoku na systém zamykání a odemykání automobilu, se řešení týká spíše mechanického zabezpečení. Vzhledem k velmi častému výskytu těchto útoků se začal používat systém VAM, který by měl automobil dostatečně ochránit. Tento systém si ovšem musí uživatel vozidla zakoupit. Pro proces kybernetického útoku na multimediální systém bylo navrženo možností více. První možností je zabezpečení pomocí antivirů instalovaných do těchto systémů, příkladem je program ECUShield. Druhou možností je využití program k šifrování dat a třetí možnost zabezpečení z hlediska kybernetické bezpečnosti spočívá v pravidelných softwarových aktualizacích. Tyto aktualizace byly sice k dispozici neustále, ale spousta uživatelů je nevyužívala, protože bylo nutné navštívit s automobilem autoser-

vis, kde tyto aktualizace provedli odborníci. Dalo by se tedy říct, že tento způsob ochrany není uživatelsky přátelský. Společnost Continental proto přichází s řešením, kdy bude možné tyto softwary aktualizovat, takřka z pohodlí domova, pomocí mobilních telefonů. Na Světovém mobilním kongresu, který se konal na začátku roku 2018, představila tato společnost svou vizi o tom, jak tato proměna ovlivní automobily v budoucnosti.

V dnešní době plné moderních technologií je nutné si připustit, že riziko kybernetických útoků je všude kolem nás. Domníváme se, že by proto měl být kladen větší důraz i na kybernetickou bezpečnost. Ať už jde o nebezpečí kybernetických útoků na automobily, kterým se věnuje tato bakalářská práce, nebo o kybernetické útoky na kterékoli jiné oblasti, rizika se zvyšují zároveň s vývojem technologií. Předkládaná práce si nekladla za cíl pokrýt téma kybernetické bezpečnosti celkově, má být spíše dílčím příspěvkem k diskuzi o této problematice, která si bezpochyby vyžaduje další zkoumání. Tato práce může také sloužit jako východisko při další práci zaměřené na podobnou či totožnou problematiku.

SEZNAM POUŽITÉ LITERATURY

[1] ATSMON, Alon. Multilayered cybersecurity architecture and suite. In: *GENIVI Open Source Projects Wiki* [online]. 2016 [cit. 2018-05-07]. Dostupné z: https://at.projects.genivi.org/wiki/display/WIK4/14th+GENIVI+AMM

[2] BEDNÁŘ, Marek. ECUShield: „antivir" pro auta má z vozu udělat pro hackery nedobytnou pevnost. In: *autoforum.cz*[online]. 2015 [cit. 2018-05-07]. Dostupné z: http://www.autoforum.cz/predstaveni/ecushield-antivir-pro-auta-ma-z-vozu-udelat-pro-hackery-nedobytnou-pevnost/

[3] BEDNÁŘ, Marek. Takhle se dnes kradou auta, bezklíčový vstup je otevře každému. In: *autoforum.cz*[online]. 2015 [cit. 2018-05-07]. Dostupné z: http://www.autoforum.cz/zivot-ridice/takhle-se-dnes-kradou-auta-bezklicovy-vstup-je-otevre-kazdemu/

[4] BORSKÝ, Daniel. Trendy moderní doby: Multimediální systém. In: *autickar.cz* [online]. 2016 [cit. 2018-03-19]. Dostupné z:https://www.autickar.cz/clanek/centralni-mozek-auta/

[5] BUREŠ, David. Auta lze pořád ukrást za pár sekund. Díky signálu z bezklíčového odemykání. In: *auto.cz*[online]. 2017 [cit. 2018-05-07]. Dostupné z: http://www.auto.cz/auta-lze-porad-ukrast-za-par-sekund-diky-signalu-z-bezklicoveho-odemykani-109161

[6] Další a snadný cíl hackerů - auta, ©2014-2018. *SECURITY MAGAZÍN* [online]. Security Media [cit. 2018-04-09]. Dostupné z: https://www.securitymagazin.cz/technologie/automobilky-nejsou-schopne-ochranit-auta-pred-utoky-hackeru-1404043723.html

[7] DORDA, Michal. Úvod do modelování a simulace systémů. In: *HomeL – Informace a materiály pro studenty* [online]. [b.r.] [cit. 2018-01-28]. Dostupné z: http://homel.vsb.cz/~dor028/Aplikace_2.pdf

[8] ECU – Engine Control Unit. In: *Zákruta.cz*[online]. [b.r.][cit. 2018-04-09]. Dostupné z: http://www.zakruta.cz/slovnik-pojmu/pojem/ecu/

[9] ECUSHIELD. In: *Harman a Samsung Company*[online]. © 2012 – 2018 [cit. 2018-05-07]. Dostupné z: http://tower-sec.com/ecushield/

[10] FEJTKOVÁ, Petra. Potřebuji dělat výzkum: jaké kroky udělat a proč. In: *Petra Fejtková*[online]. [b.r.] [cit. 2018-05-01]. Dostupné z: http://petrafejtkova.cz/blog/14-faze-vyzkumu-jejich-vyznam

[11] Firmware. In: *ITslovník.cz* [online]. © 2008 - 2018[cit. 2018-04-09]. Dostupné z: https://it-slovnik.cz/pojem/firmware

[12] FUGLEVIČ, Daniel. Jak se chránit před zloději aut s bezklíčovým ovládáním? Řešení máte v kuchyni. In: *Automix.cz* [online]. 2018 [cit. 2018-05-07]. Dostupné z: https://automix.cars.cz/zivot-ridice/jak-se-ochranit-pred-zlodeji-hackery-aut-reseni-hledejte-v-kuchyni-20180419.html

[13] GREENBERG, Andy. HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT. In: *Wired.com* [online]. 2015 [cit. 2018-05-09]. Dostupné z:https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[14] HRŮZA, Petr. *Kybernetická bezpečnost II*. Brno: Univerzita obrany, 2013. ISBN 978-80-7231-931-2.

[15] Jak se vyhnout krádeži auta, zloději už nepotřebují páčidlo, ale špičkovou elektroniku. In: *mBenzin.cz* [online]. 2017 [cit. 2018-05-07]. Dostupné z: https://www.mbenzin.cz/Clanky/Jak-se-vyhnout-kradezi-auta-zlodeji-uz-nepotrebuji-pacidlo-ale-spickovou-elektroniku-A_7415

[16] KERNER, Sean Michael, 2017. Hyundai Mobile AppPatchedfor Car Hacking Vulnerabilities. EWeek [online]. 1-1 [cit. 2018-05-02]. ISSN 15306283. Dostupné z: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&an=122732892&scope=site

[17] KESSY - Bezklíčový přístup a startování vozu. In: *smucler.cz* [online]. 2017 [cit. 2018-03-19]. Dostupné z:https://www.smucler.cz/blog/kessy-bezklicovy-pristup-a-startovani-vozu/

[18] KLAMO, Matej. Ford přichází s novým komunikačním systémem Sync. In: *Auto-Revue.cz*[online]. 2008 [cit. 2018-05-01]. Dostupné z: https://www.autorevue.cz/ford-prichazi-s-novym-komunikacnim-systemem-sync_2

[19] KOHOUT, Martin. Continental chrání automobilové komponenty a výrobní závody proti hacku. In: *freebit.cz* [online]. 2018 [cit. 2018-05-07]. Dostupné z: https://freebit.cz/continental-chrani-automobilove-komponenty-a-vyrobni-zavody-proti-hacku/

[20] Kyberzločin na silnici: automobilky zanedbaly ochranu před hackery.In: *Euro.cz* [online]. 2017 [cit. 2018-05-07]. Dostupné z: https://www.euro.cz/byznys/kyberzlocin-na-silnici-automobilky-zanedbaly-ochranu-pred-hackery-1378774

[21] Mapa procesů (Process Map). In: *ManagementMania.com*[online]. 2016[cit. 2018-01-29]. Dostupné z: https://managementmania.com/cs/mapa-procesu

[22] MILER, Petr. Takhle vypadal palubní počítač auta v roce 1983. Uměl i něco, co ty dnešní ne. In: *AutoForum.cz*[online]. 2018 [cit. 2018-05-01]. Dostupné z: http://www.autoforum.cz/fascinace/takhle-vypadal-palubni-pocitac-auta-v-roce-1983-umel-i-neco-co-ty-dnesni-ne/

[23] Multimediální referenční systém Bosch. In: *MotoFocus.cz*[online]. 2009 [cit. 2018-05-01]. Dostupné z: https://motofocus.cz/vyrobci/123,multimedialni-referencni-system-bosch

[24] Olympijské hry v Pchjongčchangu jsou pod útoky hackerů. In: *České tech.intory.cz* [online]. 2018 [cit. 2018-05-01]. Dostupné z: http://tech.instory.cz/250-olympijske-hry-v-pchjongcchangu-jsou-pod-utoky-hackeru.html

[25] PLŮCHA, Martin. Informační a komunikační systémy. In: *automobilové-systemy.wz.cz* [online]. 2012 [cit. 2018-03-19]. Dostupné z:http://www.automobilove-systemy.wz.cz/infosystemy.html

[26] POŽIVIL, Jaroslav, Bohumil BERNAUER a Tomáš VANĚK. *Procesní systémové inženýrství*. Praha: Vysoká škola chemicko-technologická, 1997, 220 s. ISBN 80-708-0311-8.

[27] Procesní management. In: *Krajská hospodářská komora Královéhradeckého kraje* [online]. [b.r.] [cit. 2018-01-29]. Dostupné z: http://www.komora-khk.cz/business/documents/?soubor=moduly/5-jakost/06-procesni-model-systemu-managementu-jakosti/06-procesni-management.pdf

[28] RADVAN, Ladislav. Sběrnice CAN (Controller Area Network). In: *MIKROKONTROLÉRY INFINEON TECHNOLOGIES* [online]. [b.r.] [cit. 2018-04-09]. Dostupné z: http://noel.feld.cvut.cz/vyu/scs/prezentace2002/Infineon/can.htm

[29] Remotekeylesssystem. In: *Wikipedia: the free encyclopedia*[online]. 2018 [cit. 2018-05-01]. Dostupné z: https://en.wikipedia.org/wiki/Remote_keyless_system

[30] SEINER, Zdeněk. Revoluční automobilové odemykání vymysleli v Přelouči, nepotřebuje klíč. In: *Novinky.cz*[online]. 2015 [cit. 2018-05-01]. Dostupné z:

https://www.novinky.cz/auto/364371-revolucni-automobilove-odemykani-vymysleli-v-prelouci-nepotrebuje-klic.html

[31] SOUČEK, Vladimír a Eva STAŇOVÁ a Martin LINHART. Vnitřní bezpečnost a veřejný pořádek, Krizové řízení. In: *mvcr.cz* [online]. Praha 2005 [cit. 2018-05-07]. Dostupné z: www.mvcr.cz/soubor/bezpecnost-pdf.aspx

[32] STŘELEC, Jiří. Modelování procesů. In: *VlastníCesta.cz* [online]. 2012[cit. 2018-01-28]. Dostupné z: http://www.vlastnicesta.cz/metody/modelovani-procesu/

[33] Svět zasáhla další vlna kybernetických útoků, dostala se i do ČR. In: *České noviny.cz* [online]. 2017 [cit. 2018-05-01]. Dostupné z: http://www.ceskenoviny.cz/zpravy/svet-zasahla-dalsi-vlna-kybernetickych-utoku-dostala-se-i-do-cr/1501449

[34] ŠEBEK, Václav. Řízení projektů a podnikových procesů: Modelování procesů. In: *SlidePlayer* [online]. © 2018 [cit. 2018-01-30]. Dostupné z: http://slideplayer.cz/slide/4196952/

[35] ŠEFČÍK, Vladimír a Jiří KONEČNÝ. *Procesní inženýrství: bezpečné a spolehlivé vedení procesů.* Uherské Hradiště [i.e. Ve Zlíně]: Univerzita Tomáše Bati ve Zlíně, 2013, 106 s. ISBN 978-80-7454-280-0.

[36] Volvo půjde odemknout bez klíče prostřednictvím mobilu. In: *Týden.cz*[online]. 2016 [cit. 2018-05-01]. Dostupné z: https://www.tyden.cz/rubriky/auta/zajimavosti/volvo-pujde-odemknout-bez-klice-prostrednictvim-mobilu_373073.html

[37] Vývojový diagram (Flow chart). In: *ManagementMania.com*[online]. 2017[cit. 2018-01-29]. Dostupné z: https://managementmania.com/cs/vyvojovy-diagram-flow-chart

[38] Výzkumy.knihovna.cz [online]. Brno, © 2012 [cit. 2018-05-01]. Dostupné z:http://vyzkumy.knihovna.cz/

[39] What is a Process Engineer?. In: *GetReskilled.com*[online]. © 2018 [cit. 2018-01-30]. Dostupné z: http://www.getreskilled.com/what-is-a-process-engineer/

[40] Zabezpečení auta proti krádeži: na jaký systém se můžete s jistotou spolehnout? In: *Autojournal.cz* [online]. 2018 [cit. 2018-05-07]. Dostupné z: http://www.autojournal.cz/zabezpeceni-auta-proti-kradezi-na-jaky-system-se-muzete-s-jistotou-spolehnout/

[41] Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů. In: *Zakonyprolidi.cz* [online]. [cit. 2018-03-22]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

[42] Zavirování automobilu přes internet. In: *Viry.cz* [online]. 2015 [cit. 2018-05-09]. Dostupné z:https://www.viry.cz/zavirovani-automobilu-pres-internet/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ADAC	Allgemeiner Deutscher Automobil Club
AVB	Audio Video Bridging
CAN	Controller Area Network
ECU	Engine Control Unit
ERM	Entity Relationship Model
GPS	Global Positioning System
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
JTAG Tools	Joint Test Action Group
KESSY	Keyless Entry, Start and exit System
MOST	Media Oriented Systém Transport
USB	Universal Serial Bus

SEZNAM OBRÁZKŮ

Obr.1. Znázornění procesu 14
Obr.2. Vývojový diagram přístupu k procesnímu inženýrství 16
Obr.3. Symboly vývojového diagramu 23
Obr.4. Fáze výzkumu 24
Obr.5. Graf zastoupení pohlaví respondentů 28
Obr.6. Graf věkového složení respondentů 28
Obr.7. Graf povědomí o kybernetickém útoku na automobil 29
Obr.8. Graf vyhodnocení názorů respondentů ohledně zabezpečení automobilů 30
Obr.9. Potential attack surfaces 38
Obr.10. Proces napadení kybernetického systému zamykání a odemykání vozidla 40
Obr.11. Proces napadení automobilu přes multimediální systém 41
Obr.12. Systémové pojetí problematiky kybernetického útoku na systémy v automobilu, ... 44

SEZNAM TABULEK

Tab.1. Test závislosti rizikovosti na pohlaví při kybernetickém útoku na multimediální systém v automobilu 31
Tab.2. Chí - kvadrát test..... 32
Tab.3. Test závislosti rizikovosti na pohlaví při kybernetickém útoku na systém zamykání a odemykání automobilu 33
Tab.4.Chí – kvadrát test..... 33
Tab.5. Test závislosti rizikovosti na věku při kybernetickém útoku na multimediální systém v automobilu 34
Tab.6. Chí – kvadrát test..... 35
Tab.7. Test závislosti rizikovosti na věku při kybernetickém útoku na multimediální systém v automobilu 36
Tab.8. Chí – kvadrát test..... 36

SEZNAM PŘÍLOH

P I Zdroje použité v analýze informačních zdrojů

P II Seznam testovaných automobilů

P III Dotazník

PŘÍLOHA PI: ZDROJE POUŽITÉ V ANALÝZE INFORMAČNÍCH ZDOJŮ

BALÁŽIK, Milan. Reakce a obrana proti kybernetickým útokům v prostředí SCADA. *Systemonline.cz* [online]. 2014, s. 22 [cit. 2018-05-08]. ISSN 1802-615X. Dostupné z: https://www.systemonline.cz/rizeni-vyroby/reakce-a-obrana-proti-kybernetickym-utokum-v-prostredi-scada.htm

BASTL, Martin a Zuzana GRUBEROVÁ. Kyberprostor jako „pátá doména"?.*Vojenské rozhledy*[online]. Praha: Ministerstvo obrany České republiky, 2013, 22(4), s. 10-21 [cit. 2018-01-30]. ISSN 1210-3292. Dostupné z:http://www.vojenskerozhledy.cz/kategorie-clanku/bezpecnostni-prostredi/kyberprostor-jako-pata-domena

HROMADA, Martin et al., 2015. *Kybernetická bezpečnost: teorie a praxe*. Praha: Powerprint. ISBN 978-808-7994-726.

CHIOCK, Mario a RODILLAS, Del . Kybernetická bezpečnost průmyslových řídicích systémů (část 1). In: *Automa.cz* [online]. 2015 [cit. 2018-05-01]. Dostupné z: http://www.automa.cz/cz/web-clanky/kyberneticka-bezpecnost-prumyslovych-ridicich-systemu-cast-1-54542_7659/

CHOI, Lin V. a Eric A. FISCHER, c2005. *Cybersecurity and homelandsecurity*. New York: Nova Science Publishers. ISBN 978-159-4547-287.

iCTDay – Bezpečnost kyberprostoru. In: *Stech.cz* [online]. 2012 [cit. 2018-05-07]. Dostupné z: http://www.stech.cz/konference/archiv/prednasky-z-konferenci-sdelovaci-techniky-2012/ict-day.aspx

Konference Cíl a cesta ke kybernetické bezpečnosti nejen v mezích zákona. In: *Nsmcluster.com* [online]. 2015 [cit. 2018-05-07]. Dostupné z: http://www.nsmcluster.com/konference/

Konference o kybernetické bezpečnosti a smart grids. In: *Automa.cz* [online]. 2011 [cit. 2018-04-28]. Dostupné z: http://automa.cz/cz/casopis-clanky/konference-o-kybernetickebezpecnosti-a-smart-grids-2011_10_44471_4861/

Konference o kybernetické bezpečnosti. In: *GDPRSystems.cz* [online]. 2017 [cit. 2018-05-07]. Dostupné z: https://gdprsystems.cz/2017/06/26/konference-o-kybernetické-bezpecnosti/

KOSTOPOULOS, George K., 2017. *Cyberspace and cybersecurity*. Second edition. BocaRaton: CRC Press. ISBN 978-131-5116-488.

Kybernetická bezpečnost: o čem je nový zákon?. In: *root.cz* [online]. 2015 [cit. 2018-03-20]. Dostupné z: https://www.root.cz/clanky/kyberneticka-bezpecnost-o-cem-je-novy-zakon/

LOUCKÝ, Milan. Kybernetická bezpečnost a vize do 2017. *ICT Network News.com* [online]. 2016, 11-12, s. 1 [cit. 2018-05-07]. Dostupné z: http://ict-nn.com/data/magaziny/bul-1480493489-5.pdf

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). In: *govcert.cz* [online]. 2018 [cit. 2018-04-29]. Dostupné z: https://www.govcert.cz/

NĚMEC, Marian. Vím, že nic nevím - pro kybernetickou bezpečnost bohužel platí známé Sokratovo úsloví. *Systemonline.cz* [online]. 2017, s. 06 [cit. 2018-05-08]. ISSN 1802-615X. Dostupné z: https://www.systemonline.cz/clanky/kybersvet-je-nebezpecne-misto.htm

PORADA, Viktor. *Kriminalistika: Technické, forenzní a kybernetické aspekty.* Plzeň: Aleš Čeněk, 2016, 1024 s. ISBN 978-80-7380-589-0.

Řízení procesů a aplikace moderních technologií – Kybernetická bezpečnost. In: *e-konference.utb.cz* [online]. 2018 [cit. 2018-05-07]. Dostupné z: https://e-konference.utb.cz/

SINGER, P. W., 2014. *Cybersecurity and cyberwar: whatevery one needs to know*. New York: Oxford University Press. ISBN 978-019-9918-119.

ŠAVEL, Jindřich. Kybernetická bezpečnost: Co s tím?. *Komora: Společník ve světě podnikání a průmyslu*[online]. Praha:Hospodářská komora České republiky, 2016, 17(11), s. 42-43 [cit. 2017-12-13]. ISSN 1802-1247. Dostupné z:http://www.cotmedia.cz/ecasopisy/komora/2016/1116/files/assets/basic-html/index.html#42

The Community's Official Cybersecurity Conferences Directory For 2018. In: *Infosec-conferences.com* [online]. 2018 [cit. 2018-04-08]. Dostupné z: https://infosec-conferences.com/

PŘÍLOHA P II: SEZNAM TESTOVANÝCH AUTOMOBILŮ

Seznam aut, na nichž ADAC testoval podvodné odemknutí a nastartování pomocí bezklíčového odemknutí	
Značka	Model
Alfa Romeo	Giulia
Audi	Q2, A3, A4, A4 Avant, A5, A6, A6 allroad, R8, SQ 7, TT RS, TT S
BMW	225xe, 318i, 318d, 440i GC, 520d, 520d Touring, 640d, 730d, 740, 740d, i3, X1
Citroën	DS 4 CrossBack, C3, C4 Picasso, SpaceTourer
Fiat	124 Spider
Ford	EcoSport, Edge, Focus, RS, Galafy, Kuga, Mustang, S-Max
Honda	HR-V
Hyundai	i10, i30, i40, Ioniq, ix35, Santa Fe
Infiniti	Q30
Jaguar	F-Pace
Kia	Niro, Optima
Land Rover	Discovery, Evoque
Lexus	RX
Mazda	3, CX-5, MX-5
Mercedes-Benz	E
Mini	Clubman, Cabrio, Countryman
Mitsubishi	Outlander, Space Star
Nissan	Leaf, Micra, Navara, Qashqai, Qashqai+2
Opel	Ampera, Ampera-E, Astra
Peugeot	508, 3008, 5008
Renault	Captur, Clio, Grand Scénic, Kadjar, Mégane, Scénic, Talisman, Traffic
Seat	Ateca, Leon
Škoda	Kodiaq, Octavia, Superb
SsangYong	Tivoli
Suzuki	SX4, Baleno, Swift, Vitara
Subaru	Levorg
Tesla	Model S
Toyota	C-HR, Mirai, Prius, RAV4, Verso
Volvo	V40, S90, V90, XC90
Volkswagen	Golf, Passat, Tiguan, Touran
Pozn. Naprostá většina vyrobených aut byla vyrobena mezi lety 2015 až 2017, vybrané modely jsou i staršího data výroby, nejstarší je Toyota Prius z roku 2007.	

PŘÍLOHA P III: DOTAZNÍK

Dotazník na téma kybernetických útoků na automobil

Dobrý den jsem studentkou posledního ročníku bakalářského studia oboru Ovládání rizik. Chtěla bych Vás tímto poprosit o vyplnění dotazníku k praktické části mojí bakalářské práce. Jedná se především o kybernetickou bezpečnost. Dotazník je konkrétně vztažen na kybernetické útoky na vozidla. Myslím si, že v dnešní moderní době a čím dál větší modernizaci automobilů, je otázkou času, kdy se takové útoky stanou běžnou záležitostí. Dotazník je zcela anonymní a slouží pouze k účelům mojí BP.

*Povinné pole

Pohlaví *

- ○ Muž
- ○ Žena

Věk *

- ○ 18-28
- ○ 29-39
- ○ 40 a více

Jste aktivním řidičem? *

- ○ Ano
- ○ Ne

Napadlo Vás, že automobil, který řídíte může být cílem útoku hackera? *

- ○ Ano
- ○ Ne

Setkali jste se někdy s takovým útokem, ať už máte osobní zkušenost nebo zkušenost někoho v okolí? *

- ○ Ano
- ○ Ne

Myslíte si, že jsou současné moderní automobily dostatečně zabezpečeny proti takovým útokům? *

- ○ Ano
- ○ Ne

Nastane-li situace, že útočník napadne Váš automobil, ohodnoťte, který kybernetický útok Vás může nejvíce ohrozit na životě od 1 (nejmenší riziko) do 5 (největší riziko): *

	1	2	3	4	5
Kybernetický útok na multimediální systém	○	○	○	○	○
Útok na systém zamykání a odemykání automobilu	○	○	○	○	○

ODESLAT