Sociální inženýrství v průmyslu komerční bezpečnosti
Social engineering in the industry of commercial security

Adam Polášek

Bakalářská práce
2016

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2015/2016

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Adam Polášek**
Osobní číslo:	**A13634**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Sociální inženýrství v průmyslu komerční bezpečnosti**
Téma anglicky:	**Social Engineering in the Commercial Security Industry**

Zásady pro vypracování:

1. **Seznamte se s problematikou sociálního inženýrství.**
2. **Definujte základní pojmy sociálního inženýrství.**
3. **Specifikujte jeho využitelnost v průmyslu komerční bezpečnosti.**
4. **Navrhněte sociální experiment zaměřený na vyzrazení citlivých informací.**
5. **Zrealizujte a vyhodnoťte navrhovaný experiment.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **EKMAN, Paul. Odhalené emoce. Jan Melvil Publishing, 2015. ISBN 9788087270813.**
2. **NAVARRO, Joe a Marvin KARLINS. Jak prokouknout druhé lidi: Příručka bývalého experta FBI. Grada, 2010. ISBN 978-80-247-3350-0.**
3. **EKMAN, Paul. Emoce pod maskou. BIZBOOKS, 2015. ISBN 9788026504221.**
4. **MITNICK, Kevin a William SIMON. Umění klamu. HELION, 2003. ISBN 83-7361-210-6.**
5. **CIALDINI, B. Robert. Zbraně vlivu. Jan Melvil Publishing, 2012. ISBN 978-80-87270-32-5.**

Vedoucí bakalářské práce: **Ing. Dora Lapková**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **23. února 2016**

Termín odevzdání bakalářské práce: **30. května 2016**

Ve Zlíně dne 16. února 2016

doc. Mgr. Milan Adámek, Ph.D.
děkan

L.S.

Ing. Jan Valouch, Ph.D.
ředitel ústavu

Prohlašuji, že

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

Prohlašuji,

- že jsem na diplomové/bakalářské 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 16. 5. 2016

Adam Adámek
.....
podpis diplomanta

ABSTRAKT

Bakalářská práce je zaměřená na problematiku sociálního inženýrství v průmyslu komerční bezpečnosti, objasnění základních pojmů spojených se sociálním inženýrstvím a využití sociálního inženýrství v průmyslu komerční bezpečnosti. Teoretická část je zaměřena na neverbální komunikaci, která je úzce spjata se sociálním inženýrstvím. Jsou zde objasněny základní pojmy týkající se neverbální komunikace, dále projevy neverbální komunikace a emocí. Praktická část se zaměřuje na zhotovení sociálního experimentu. Cílem sociálního experimentu bylo zjistit, do jaké míry jsou lidé schopni prozradit citlivé informace prostřednictvím dotazníků.

Klíčová slova: Sociální inženýrství, metody sociálního inženýrství, experiment, neverbální komunikace, Ekman

ABSTRACT

The bachelor thesis is focused on the issue of social engineering in the commercial security industry, the clarification of the basic terms related to social engineering and the using of social engineering in the commercial security industry. The theoretical part is focused on non-verbal communication, which is closely associated with social engineering. The basic concepts relating to non-verbal communication, nonverbal communication, speech and emotions are explained there. The practical part is focused on making a social experiment. The aim of the social experiment was to determine if the people are able to disclose sensitive information via questionnaires and to what extent.

Keywords: Social engineering, methods of social engineering, experiment, nonverbal communication, Ekman

Chtěl bych poděkovat mé vedoucí bakalářské práce **Ing. Doře Lapkové** za její čas a trpělivost při konzultacích ohledně bakalářské práce. Za její vstřícnost, ochotu a hromadu cenných informací, které jsem zúročil při vypracovávání bakalářské práci. Dále bych chtěl poděkovat své rodině, která mi byla oporou. Také bych chtěl poděkovat panu **Martinu Balážovi** za poskytnutí cenných informací, které vedly k dokončení bakalářské práce. Velké díky patří také všem lidem, kteří ochotně vyplnili mé dotazníky.

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

OBSAH

ÚVOD

Sociální inženýrství je v dnešní době chápáno jako internetová hrozba. Nemusí však vždy být tato hrozba uskutečněná přes internet. Je mnoho technik a způsobů, jak promítnout sociální inženýrství do reálného života. Tyto techniky jsou buď vědomě, nebo nevědomě využívány nejenom v průmyslu komerční bezpečnosti, ale obecně všemi lidmi. S pojmem sociální inženýrství souvisí neverbální komunikace, která tvoří její nedílnou část. Neverbální komunikace jako celek je klíčová pro to, aby člověk s použitím příslušné techniky sociálního inženýrství mohl tuto techniku efektivně využít. V dnešní době můžeme mít jakkoli dobré zabezpečení, ale obecně je pořád jejím nejslabším prvkem lidský faktor. V mnoha případech se dá lidský faktor velmi snadno ovlivnit.

Cílem bakalářské práce je seznámit s problematikou sociálního inženýrství a definovat základní pojmy spojené se sociálním inženýrstvím. V rámci práce bude ukázána využitelnost sociálního inženýrství v průmyslu komerční bezpečnosti. V neposlední řadě bude navrhnut, realizován a vyhodnocen sociální experiment zaměřený na vyzrazení citlivých informací prostřednictvím dotazníků.

Teoretická část bakalářské práce je zaměřena na sociální inženýrství, na pojmy spojené se sociálním inženýrstvím, historii a techniky, které se v současné době v sociálním inženýrství používají. Důležitá část jsou také obvyklé typy útoků sociálního inženýrství, které se používají přes internet. Je zde vysvětlen rozdíl mezi sociálním inženýrstvím, které probíhá přes internet a které využívá kontaktu s lidmi. Další kapitolou jsou metody sociálního inženýrství. Sociální inženýrství je spojeno s neverbální komunikací. Je zde vysvětlen pojem neverbální komunikace, a jakým způsobem se dá neverbální komunikace využít v praxi. Další nedílnou součástí neverbální komunikace jsou její projevy a emoce. Jsou zde vysvětleny pojmy, které se pojí s neverbální komunikací, dále jsou vysvětleny a ukázány základní projevy emocí. V poslední kapitole teoretické části je naznačeno využití sociálního inženýrství v průmyslu komerční bezpečnosti. Je zde uveden rozhovor s panem Martinem Balážem, který objasnil, jakým způsobem se neverbální komunikace využívá u policie.

Praktická část je zaměřená na sestavení vhodného dotazníku pro účely sociálního experimentu. Sociální experiment má za úkol zjistit, do jaké míry jsou lidé schopni prozradit citlivé informace prostřednictvím dotazníků a na to, jakým způsobem se dají dotazníky zneužít ve prospěch pachatele. Sociální experiment se skládá ze dvou dotazníků, které byly rozšířeny jak ve formě elektronické, tak ve formě písemné.

I. TEORETICKÁ ČÁST

1 SOCIÁLNÍ INŽENÝRSTVÍ

Sociální inženýrství je umění manipulace s lidmi, kteří následně prozradí důvěrné informace na sebe nebo na své známé. Druhy informací, o které se tito pachatelé zajímají, se ve většině případů liší. Pokud se však útočník zaměří přímo na jednotlivce, snaží se vás přimět, abyste mu dali své heslo nebo informace o bankovním účtu. Nebo také přístup do vašeho počítače pomocí nainstalovaného škodlivého softwaru, který mu přístup poskytne. O škodlivém softwaru nemusí uživatel ani vědět. Skrze škodlivý software si pachatel zjistí informace, např. o bankovním učtu, hesla nebo převezme kontrolu nad počítačem.

Zločinci používají taktiky sociálního inženýrství, protože je obvykle snazší zatlačit na přirozenou náturu člověka než vymýšlet software, kterým by se nabourali do zabezpečeného systému. Například je dokázané, že je jednodušší člověka oklamat k tomu, aby sdělil své heslo, než se obvykle těžším způsobem snažit heslo nabourat (samozřejmě pokud to heslo není jednoduché). [1]

Bezpečnost je o tom, komu můžeme věřit a rozlišit mezi tím co je a co není pravda. Vědět kdy ano a kdy ne. Kdy věřit, že člověk, se kterým komunikuji, je opravdu člověk, se kterým si myslím, že komunikuji. Kdy věřit, že webová stránka je nebo není důvěryhodná. Kdy věřit, že člověk na druhé straně telefonu je důvěryhodný. Kdy a kde je bezpečné sdělovat informace.

Kdybychom se zeptali kohokoli, kdo se pohybuje v bezpečnostním odvětví na otázku, co je nejslabším článkem obecně v bezpečnostním odvětví, tak všichni odpoví, že je to lidský faktor. Nezaleží na tom, kolik zámků a dalších bezpečnostních překážek máme na dveřích a oknech nebo pokud máme hlídacího psa, poplachový systém, žiletkové plochy a ozbrojenou ochranku. Pokud věříme člověku, který se u brány legitimuje jako donašeč pizzy a pustíme ho dovnitř bez toho, aniž bychom ho zkontrolovali (proč, když nese jenom pizzu), potom jsou veškeré bezpečnostní prvky k ničemu.[2]

1.1 Historie

Sociální inženýrství je v dnešní spojováno s hrozbami, se kterými se člověk může setkat pouze na internetu. Opak je pravdou, sociální inženýrství se datuje už od roku 1600, kde George Psalmanazar falešně prohlašoval, že je první Formosan, který navštívil Evropu. Dokonce v té době napsal první knihu o Evropě, kterou vydal v provincii Formosa, která leží na severovýchodě Argentiny. George Psalmanazar je považován za jednoho z prvních sociálních inženýrů.

Další z řady sociálních inženýru je Viktor Lustig původem z Česka, který se proslavil jako „Muž, který prodal Eiffelovu věž. Dvakrát“. Po první světové válce v roce 1925 Lustig využil příležitosti, kdy se ve Francii spekulovalo o tom, že se Eiffelova věž přestěhuje, protože je nákladná a nesplývá s ostatními památkami tehdejší Francie. Lustig pod hlavičkou ředitele Ministerstva pošty a telegrafů rozeslal pozvánky šesti významným obchodníkům s kovošrotem a pozval je na schůzku k projednání malého obchodu. Na schůzce jim řekl, že Eiffelova věž nesplnila představy a že byl pověřen její likvidací. Všechno bylo schváleno a nakonec Lustig inkasoval peníze za prodanou Eiffelovu věž i s úplatkem, který mu dal jeden z obchodníků.

Dalším významným představitelem sociálního inženýrství je Kevin Mitnick, který jako první kombinoval sociální inženýrství jak přes internet, tak konfrontací s fyzickými osobami. Již ve dvanácti letech cestoval autobusem do školy zadarmo. Po rozhovoru s řidičem autobusu se dozvěděl, jak funguje systém jízdenek a kam se vyhazují staré ražičky lístků. Mitnick si ražičku obstaral, a tak cestoval po Los Angeles v té době zadarmo. Svoji první zkušenost s drátovými systémy poznal na střední škole, kde ho spolužák zasvětil do tajů telefonování, které se v tehdejší době začalo rozmáhat. V 17i letech byl Mitnick natolik zručný, že mu nedělalo problém zmanipulovat kohokoli ať už přes telefon, nebo osobně. Od telefonů se Mitnick přesunul k počítačovým sítím, kde se za pomocí sociálního inženýrství dostal do systému firem jako Nokia, Apple ale také do systémů FBI, Pentagonu, Novell. Kevin Mitnick byl zatčen v roce 1995. Byl propuštěn v roce 2000. V roce 2002 vydal knihu s názvem „Umění klamu“, kde tvrdí, že ke svým průnikům moc znalostí IT nepotřeboval. Tvrdí, že používal sociální inženýrství, vždy obsluhu dokázal přesvědčit, že ho do systému pustit má.

1.2 Obvyklé typy útoků sociálního inženýrství

Sociální inženýrství se dá rozdělit na dvě části. První část je situace, kdy pachatel musí navázat fyzický kontakt s obětí, aby mohl být útok uskutečněn a aby mohl být úspěšný.

Druhou části je pak způsob, ke kterému není třeba fyzický kontakt. Osoba tam může být zmanipulována přes internet nebo přes telefon, záleží na typu použitého útoku.

1.2.1 E-mail

Pokud se zločinci podaří, například pomocí nějaké z technik sociálního inženýrství, získat heslo k uživatelskému emailu, tak většinou získá přístup i ke kontaktům uživatele. Protože většina lidí používá všude stejné heslo, tak se pravděpodobně dostanete i ke kontaktům na sociální síti.

Pokud se zločinec jednou dostane do e-mailu uživatele, rozešle infikovaný e-mail všem jeho kontaktům. Další možností je vyvěšení odkazů na zdi sociální sítě nebo rozesílání zpráv skrze sociální sítě.

1.2.1.1 Obsahy zpráv

Zpráva může obsahovat internetový odkaz, na který podle obsahu zprávy musíte kliknout. Jelikož se zpráva tváří, jakoby byla od kamaráda a vy jste zvědaví, tak na ten odkaz kliknete. V této chvíli se vám do počítače dostane škodlivý malware, takže útočník může převzít kontrolu nad vaším počítačem a dostane se tak k vašim kontaktům. Tedy k dalším kontaktům, které může dál zneužít.

Zpráva obsahuje něco ke stažení. Může to být obrázek, hudba, video nebo třeba dokument, který má v sobě vložený škodlivý malware. Pokud přílohu stáhnete, což se ve většině případů stane, protože věříte, že je to od kamaráda, škodlivý software infikuje váš počítač. Stejně jako v předešlém příkladu, software nemusí ve všech případech zachytit antivirus. Ve většině případů uživatel ani netuší, že ho někdo naboural. V této chvíli škodlivý software odposlouchává váš počítač. [3]

1.2.2 Sociální sítě

V dnešní době jsou sociální sítě nejrozšířenější médium. Každým dnem přibývá lidí, kteří se registrují na sociální sítě a sdílí tak své soukromé informace, fotky, události. Tyto informace mohou být terčem sociálních inženýrů, kteří mohou tyto informace zneužít.

Jak již bylo výše zmíněno, pokud pachatel získá heslo uživatele a podaří se mu dostat na sociální síť např. Facebook, získá tím i přístup ke kontaktům oběti. Tudíž může začít komunikace přes Messenger s vybranými uživateli. Uživatelé jsou pak více náchylnější k tomu, aby prozradili citlivé informace pachateli, protože nemusí být zřejmé, že byl účet jejich kamaráda nabourán. Pachatel může tímto způsobem rozesílat podvodné stránky nebo infikované soubory se stejnou úspěšnosti jako u předešlého příkladu. [3]

1.2.3 Neurolingvistické programování

Dobrý sociální inženýr má dobré povědomí o tom, jak manipulovat s lidskou myslí. Neurolingvistické programování je jeden z psychologických nástrojů, pomocí kterého se sociální inženýři dostávají do lidských myslí. Pokud je tato technika použita správně, je velice účinná.

Neurolingvistické programování se opírá o neurologické procesy dané osoby, jazyk a o odezvy v chování, které si člověk od malička vypěstoval. Neurolingvistické programování bylo původně používáno psychologickými terapeuty. Sociální inženýři si určité techniky této metody vzali a přizpůsobili to svým potřebám a dalším metodám, které používali a které se stále používají.

Tato metoda se dá také jednoduše přizpůsobit sociálnímu inženýrství v průmyslu komerční bezpečnosti.

Například pokud probíhá rozhovor mezi sociálním inženýrem a obětí. Sociální inženýr se snaží přizpůsobit svůj slovník a řeč těla oběti k tomu, aby ji podvědomě zmanipuloval. Začne tím, že se bude snažit ztotožnit svoji řeč těla s řečí těla oběti. Také se bude snažit ztotožnit svoji dechovou frekvenci, hlasovou úroveň, přízvuk a slovní zásobu s danou osobou. Děláním těchto věcí si podvědomě vytváří vztah s obětí. Pak může přidat další podvědomé zprávy, tím že změní svou řeč těla, usmívá se a lehce se dotýká oběti na rameni nebo paži.

Všechny tyto hmatové, vizuální a verbální akce předávají podvědomé zprávy, které mají vliv na oběť. Pokud všechny tyto kroky zvládneme, tak můžeme přizpůsobit konverzaci tomu, co my chceme, aby oběť udělala. [4]

1.3 Techniky sociálního inženýrství

Všechny techniky sociálního inženýrství jsou založené na specifických vlastnostech lidského rozhodování známého jako kognitivní chyby v úsudku. Tyto chyby v úsudku, někdy nazývané jako "chyby v lidském hardwaru", jsou využívány mnoha způsoby k vytvoření technik sociálního inženýrství. Tyto techniky jsou rozebrány dále.

1.3.1 Pretexing

Pretexing je proces vytvoření a použití předem vymyšleného scénáře tak, aby tomu oběť věřila. Pokud příběhu oběť uvěří, je veliká šance, že sdělí potřebné informace, které by za normálních okolností neprozradila. Jde o skloubení lži s trochou pravdy. Je k tomu potřeba předchozího průzkumu, při kterém zjistíme nějakou informaci, která může být ve scénáři využitá k tomu, aby v mysli napadeného vytvořila jakýsi pocit důvěry. Na základě toho nám pak oběť může sdělit podrobnější informace nebo cokoli jiného.

Tato technika může být použita k oklamání zaměstnanců k tomu, aby sdělili soukromé informace o svých kolezích, hojně této techniky využívají soukromí detektivové nebo investigativní novináři. Mohou se tak dostat k důvěrným informacím typu telefonní číslo, bankovní účet nebo třeba telefonní záznamy.

Pretexing může být také využitý k vydávání se za spolupracovníky, policii, zástupce banky, finanční úřady, poradce v oblasti pojišťovnictví nebo jakoukoli jinou fyzickou osobu, která by mohla být v mysli oběti vnímána jako osoba důvěryhodná. Pretexer si musí jednoduše připravit odpovědi na otázky, které by mohly být obětí položeny. V některých případech stačí, aby měl pretexer dostatečně autoritativní tón hlasu a uměl improvizovat. [5]

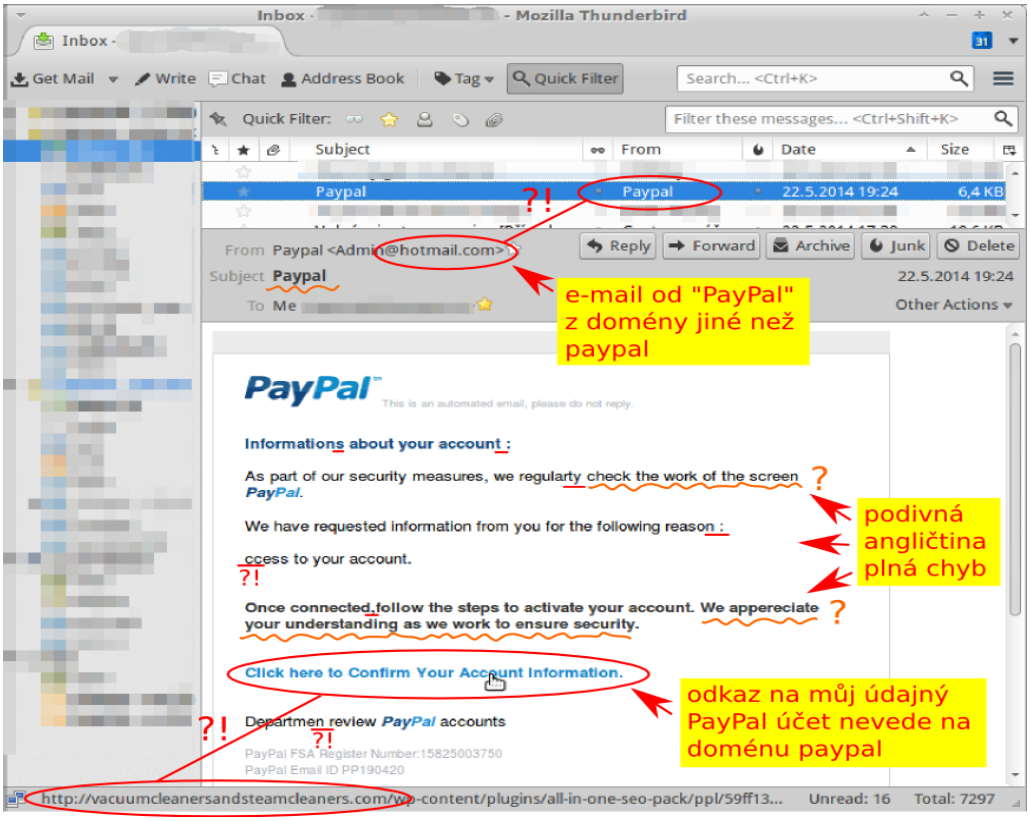
1.3.2 Phishing

Phishing je pokus o získání citlivých informací, jako jsou například hesla, uživatelská jména nebo informace o kreditní kartě za účelem dalšího zneužití. Nebo také k tomu, aby se pachatel mohl na internetu vydávat za někoho jiného.

Slovo phishing je novotvar vytvořený jako homonymum ke slovu fishing (v českém jazyce se občas používá rhybaření = rybaření), z hlediska taktiky jsou si slova velice blízká. Hodíme návnadu a čekáme, co se chytne.

Stránky a služby jako sociální sítě, aukční stránky, banky, online platby, které lidé denodenně využívají, jsou nejčastěji cílem útočníků. Phishing e-maily mohou obsahovat odkazy

na webové stránky, které jsou infikovány škodlivým softwarem. Nebo jsou odkázání na fiktivní webové stránky, které jsou identické s originálními a jsou vyzváni k zadání svých přihlašovacích údajů, které jsou následně odeslány na pachatelův e-mail. [6]



Obr. 1. Příklad podvodného emailu [7]

Phishing je příkladem techniky sociálního inženýrství, jejímž cílem je uživatele oklamat. Využívá k tomu bezpečnostních děr, které současné webové zabezpečení nepokrývá. Vzhledem k nárůstu ohlášených phishingových událostí přišla změna v právních předpisech. Přibyly školení, které mají mimo jiné za účel rozšířit povědomí lidí o takovýchto typech útoků. Přece jenom lidé jsou nejslabším článkem zabezpečení. Pokud lidé budou mít v povědomí, že tyhle typy útoků existují a budou si dávat pozor, sníží to celkový počet nejen phishingových útoků. [8]

1.3.3 Baiting

Baiting se dá přirovnat k trojskému koni v reálném světě. Tato technika využívá fyzická média, jako jsou třeba CD nebo flash disky a spoléhá na zvědavost a neostražitost oběti.

V těchto typech útoků nechávají útočníci škodlivý software uložený na přenosných fyzických úložištích. V dnešní době nejčastěji na flash discích, ale mohou to být také klasické CD nebo DVD. V minulosti se také používaly floppy disky neboli diskety.

Útočník tyto přenosné zařízení nechává na místech, kde ví, že je někdo najde. Například ve společenských místnostech, kancelářích, šatnách, výtazích nebo i na parkovišti či chodnících. Jednoduše to působí dojmem, že zařízení někdo omylem ztratil. Člověka, který takové zařízení najde, většinou nenapadne, že se jedná o tzv. bait, tudíž hned spěchá domů, aby zjistil, co se na daném zařízení nachází. Na druhé straně však útočník čeká na chvíli, kdy člověk zařízení připojí do počítače. [9]

Pokud člověk připojí nebo vloží zařízení do počítače, aby zjistil, co se na daném zařízení nachází, tak se škodlivý software může automaticky nainstalovat do počítače. V této chvílí získává útočník kontrolu nad počítačem a může si z něj vytáhnout všechny potřebné informace (hesla, e-maily, informace o bankovních účtech …). Pokud se počítač nachází v interní síti firmy, tak se útočník může jednoduše dostat dál. [10]

1.3.4 Vishing

Vishing neboli také hlasový phishing je podvodná technika sociálního inženýrství, která funguje prostřednictvím telefonu. Technika slouží k tomu, aby prostřednictvím telefonu získala z lidí na druhé straně linky důvěryhodné informace, jako například soukromé informace o bankovním účtu předem vytypované osoby nebo jeho rodné číslo, k vlastnímu prospěchu.

Vishing se opírá o důvěru veřejnosti v telefonování. V dnešní době už tato technika není tak častá záležitost, protože se v hojné míře rozmohl internet a internetové bankovnictví. Tudíž lidé začali všechny věci řešit přes internet, jak už banku, tak objednávání různých věcí apod. Najdou se ale i lidé, kteří stále důvěřují telefonu a tito lidé se stávají nejčastěji cílem útočníků. [11]

1.3.4.1 Příklad Vishingu

V červnu minulého roku 2015 zavolal Emě Watson, britské podnikatelce zřizující dětské školky, tým podvodníků, kteří se vydávali jako zástupci její banky. Oznámili jí, že na jejím účtu proběhla neobvyklá transakce, kterou se jim podařilo odchytit a že podle předpisů banky nemůžou dál manipulovat s danou částkou. Řekli jí, že její účet byl zkompromitován a požádali ji, aby peníze odeslala na podvodný účet vytvořený jejím jménem.

V policejní zprávě uvedla, že byli naprosto profesionální, že byli struční, věděli její jméno a mluvili opravdu jako zaměstnanci banky. Řekli ji, že chápou, v jaké je nešťastné situaci a že jí z této prekérní situace pomůžou, ať se ničeho nebojí.

Emma Watson přišla o 100.000£. Podvodníkům se podařilo Emmu přesvědčit, aby tyto peníze poslala na jejich fiktivní účet vedený pod jejím jménem. I přesto, že Emma nahlásila policii, co se stalo, tak se podařilo dohledat jenom zlomek z těchto peněz.

Tohle je typický příklad vishingu, kde jak bylo vidět, zločinci přesvědčili oběť, které nastínili předem vymyšlený příběh, aby jim poslala peníze na jejich fiktivní účet.

Klíčové jsou informace, tzn., že podvodníci se museli předem nachystat. Zjistili si jméno, telefonní číslo a adresu trvalého bydliště. Také si zjistili, jak vypadá skutečné spojení s bankou ohledně převádění peněz, zjistili postupy banky nebo lidí v jejich call centrech, aby byl telefonní hovor autentičtější. Dalším prvkem, který hrál v tomto případě velkou roli, byl strach, který navodili Emě, když jí řekli, že její peníze jsou ohroženy. Strach většinou vede k tomu, že lidé nepřemýšlí do důsledků a tak jednají nerozvážně.

Dále zločinci využili technologie ID spoofingu, která dovoluje zobrazit na displeji příjemce telefonní číslo podle libosti. V tomto případě to bylo telefonní číslo banky, tím zase zvýšili důvěryhodnost telefonního hovoru, protože Emma opravdu věřila, že číslo je banky.

Emma v policejní zprávě uvedla, že dokonce pozadí v telefonním hovoru znělo, jakoby někdo volal z call centra. Tím zase zvýšili důvěryhodnost telefonu, protože většinou opravdu volají pracovníci, kteří sedí v call centru. [11]

1.3.5 Quid Pro Quo

Quid Pro Quo se dá také z latiny přeložit jako „něco za něco“. Je to technika sociálního inženýrství, která se opírá o to nabídnout oběti něco za něco. Například oplatit sdělení informace nějakou jinou informací nebo dárkem. Tato sociální technika se spoléhá na důvěřivost oběti a schopnost útočníka ovlivnit oběť k tomu, aby si myslela, že výměnný obchod je výhodný.

Quid Pro Quo nastane v momentě, kdy útočník nabídne bezplatnou službu nebo dárek za informaci, kterou potřebuje. Útočník se může vydávat za IT odborníka, který bude obvolávat zaměstnance firmy do té doby, než nenajde někoho, kdo zrovna potřebuje IT pomoc. Výměnou za pomoc pak může vyžadovat nějakou informaci ba hůř, přístup do systému (např. vzdálená plocha atp.). Útočník může tvrdit, že k vyřešení problému je třeba vzdálený přístup k počítači. Oběť ochotně umožní útočníkovi vzdálený přístup k počítači výměnou za jeho opravu. Útočník se tak dostane do počítače uživatele a také v tu chvíli má přístup do celé firemní sítě. Tudíž díky tomu, že ho uživatel pustil do jeho počítače přes vzdálený přístup,

tak se útočník může dostat k citlivým informacím nejen na disku daného uživatele, ale také i k informacím, které jsou uloženy na ostatních počítačích v síti.

Quid Pro Quo technika nemusí být pouze přes internet. Byly hlášeny případy, kdy do firmy přišel člověk se soutěží o to, kdo má nejsilnější heslo. Lidé, kteří napsali své heslo, byli obdarování čokoládovou tyčinkou a propiskou. Hlavní výhra v této soutěži pro člověka, který má nejsilnější heslo, byla peněženka. Jednalo se o sociální experiment, kde bylo zjištěno, že se lidé chovají iracionálně, pokud je v soutěži nějaká materiální výhra. [12]

1.3.6 Tailgating

Tailgating, často také nazývaná piggybacking, je další ze zástupců tzv. „real world" technik sociálního inženýrství. Jedná se o techniku, kde útočník následuje osobu, která je oprávněná k přístupu do omezeného prostoru nebo do prostoru, kde je potřeba projít kontrolním stanovištěm. Tento akt může být legální či nelegální, autorizovaný nebo neautorizovaný, všechno je to v závislosti na okolnostech. Nicméně v dnešní době má tato technika spojitost spíše s nelegálním nebo s neautorizovaným vstupem.

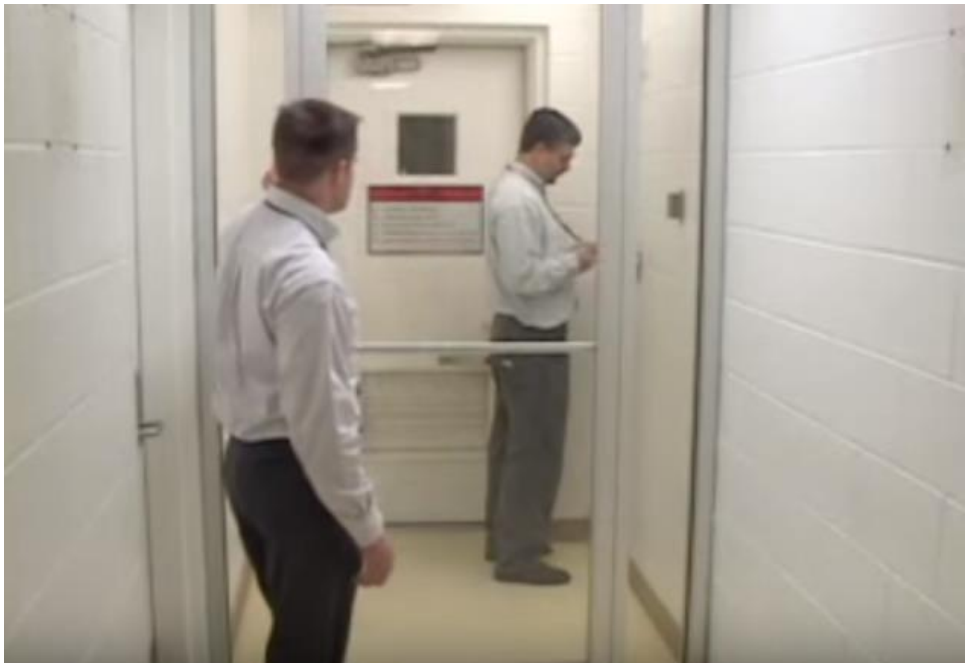
Obr. 2. Upozornění [13]

V případě, že člověk následuje osobu do prostoru, kde je vyžadována určitá kontrola nebo identifikace a aniž by o tom tato osoba věděla, tak se jedná o tailgating. Termín tailgating se

používá, pokud o tom daná osoba neví a netuší, že ji někdo bez oprávnění následuje do prostoru. Typickým příkladem tailgatingu je vstup do objektu přes dveře pomocí čipové karty. Lidé totiž většinou přiloží kartu, vstoupí do objektu, pak se již nepodívají, zda se dveře zavřou nebo zda za nimi někdo jde. V některých případech dokonce lidé dveře podrží, aby člověk, který není v těsné blízkosti za nimi, nemusel znovu přikládat čip a otevírat dveře.

Zatímco u piggybackingu se jedná o podobný proces s tím rozdílem, že člověk, který má přístup do objektu, souhlasí s tím, že člověk, který přístup nemá, může vstoupit.

Technika piggybackingu spatřila světlo světa v roce 1999. Využívali ji lidé, kteří předstírali, že jsou tajnými agenty a bez kontroly a bez lístku procházeli přes letištní kontrolu přímo do letadla. Pozdější studie ukázaly, že toho lidé zneužívali, aby na palubu letadla dostali věci, které tam nepatří, potažmo pašovali drogy nebo jiné léky do Evropy. [15]



Obr. 3. Zabezpečený vstup proti tailgatingu [14]

Na výše uvedeném obrázku je vidět, jak se v jedné americké firmě vypořádali s tailgatingem a piggybackingem. Před vstupem do chráněné oblasti jsou další dveře. Mezi těmito dveřmi se nachází přístupový systém. Přístupový systém je naprogramovaný tak, že přiložení čipové karty je možné až po zavření prvních dveří. V pomyslné místnosti, kterou tvoří dveře, je systém, který kontroluje, kolik lidí je v místnosti. Pokud jsou v místnosti dva lidé, systém vyzve, aby jeden z lidí šel před dveře a počkal, až bude na řadě. Do chráněného objektu se tedy dostane pouze člověk, který je v pomyslné místnosti sám, má čip a dveře jsou zavřené. [15]

V této kapitole jsme se dozvěděli, jaké jsou základní pojmy sociálního inženýrství. Sociální inženýrství není význam, který se vztahuje pouze na internetové podvody, jak je o tom široká veřejnost přesvědčena. Byly popsány jednotlivé techniky sociálního inženýrství. Jak techniky rozšířené přes internet, tak techniky, ke kterým je třeba navázat s člověkem komunikaci. Bylo řečeno něco málo o historii sociálního inženýrství, kde jsme se dozvěděli, že nejvýznamnějším sociálním inženýrem byl Viktor Lustig původem z Česka.

Je třeba si uvědomit, že nejslabším článkem celkového zabezpečení je lidský faktor. Můžeme mít sebelepší zabezpečení, ale použitím jakékoli výše uvedené techniky se můžeme hravě přes tato zabezpečení dostat.

2 METODY

Jak již bylo zmíněno výše, některé techniky, které se v sociálním inženýrství používají, úzce souvisí s neverbální komunikací. Neverbální komunikace se dá využít mnoha způsoby. Nejzásadnější je, že můžeme číst ostatní lidi. Díky sociálnímu inženýrství, které úzce souvisí s neverbální komunikací, můžeme člověku vnutit naši pravdu nebo ho nenápadně přinutit, aby udělal to, co chceme. Za pomocí neverbální komunikace dokážeme předpovědět reakci člověka, v kombinaci se sociálním inženýrstvím dokážeme člověka ovlivnit tak, aby nám věřil.

Díky sociálnímu inženýrství můžeme člověku vnutit svoji pravdu, důležité je však sledovat reakci člověka. Můžeme si člověka při rozhovoru jakýmsi způsobem „oťukávat“, lze tak snadno zjistit, zda míříme správným směrem k tomu, aby člověk udělal to, co chceme my nebo aby prozradil informaci, kterou potřebujeme. Každá situace může vypadat zcela jinak. Člověk, který sociální inženýrství provádí, musí vždy vědět, čeho chce použitím sociálního inženýrství dosáhnout. Může to být například nějaká informace, kterou chce, aby mu dotyčný prozradil. Sociální inženýrství může být také použito k tomu, abychom přesvědčili člověka k činu, který chceme, aby udělal.

2.1 Neverbální komunikace

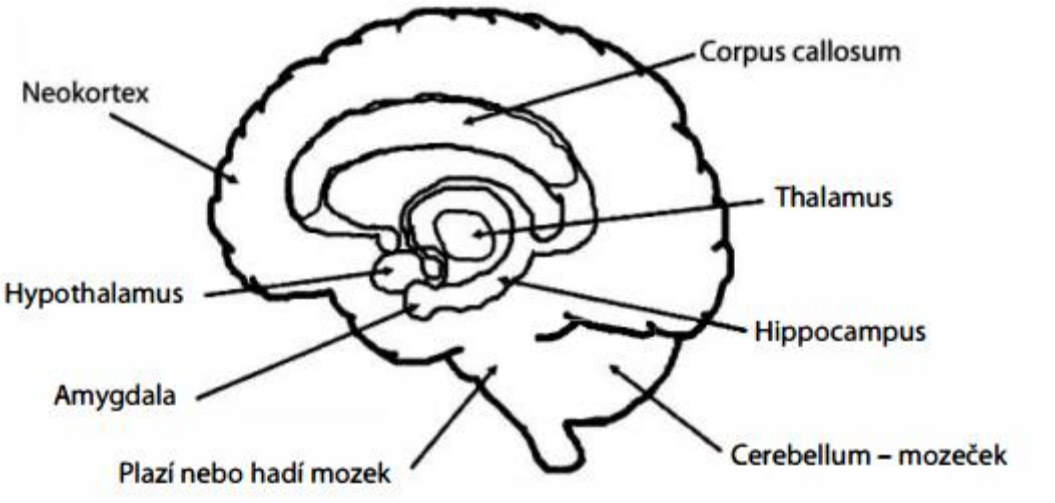
Když komunikujeme s ostatními lidmi, neustále používáme signály beze slov. Všechny naše neverbální gesta, to jak sedíme, to jak rychle nebo jak hlasitě mluvíme, jak blízko nebo jak daleko stojíme k druhé osobě, jak moc navazujeme oční kontakt. Všechny tyto zprávy, které posíláme druhé osobě, se kterou komunikujeme, mají specifický význam. Díky těmto zprávám se dá vyvodit závěr, který nám může napomoct v řešení určitých situací nebo těmto situacím předejít.

Častokrát to, co nám vychází z úst, tedy to, co říkáme, nekoresponduje s tím, jak reaguje naše tělo. Jsou to dvě odlišné věci. Při konfrontaci s těmito smíšenými signály si posluchač musí vybrat, jestli bude věřit tomu, co říkáme nebo bude spíše věřit neverbální komunikaci, která jakoby doprovází mluvený projev. Pokud vycházíme z toho, že všichni lidé lžou, zaměříme se tedy spíše na neverbální komunikaci, protože je to přirozené, je to nevědomý jazyk, který vysílá skutečné signály a pocity v jakékoli situaci. [16]

2.1.1 Jak funguje

Za to, že dáváme najevo emoce pomocí neverbální komunikace, vděčíme našemu limbickému systému, který je naším emočním centrem. Z této části mozku jdou signály do dalších částí mozku, které zase organizují naše chování spojené s emocemi nebo s přežitím. Tyto prvky dáváme najevo pomocí gest. Pokud víme, jakým způsobem se různé emoce nebo typické prvky chování v určitých situacích projevují, můžeme tyto reakce snadno přečíst a dekódovat.

Limbickou část mozku nemůžeme žádným způsobem řídit nebo ovládat, můžeme se snažit jakkoli maskovat skutečný záměr, ale čím víc se snažíme, tím více dáváme najevo pomocí gest, že něco není v pořádku, že se něco děje. [17]



Obr. 4. Schéma limbického systému [18]

Jako příklad bych uvedl událost, která se stala v Americe v prosinci roku 1999. Policie zastavila auto k namátkové kontrole. Policistka, která komunikovala s řidičem, si všimla nadměrného pocení a třasu rukou. Požádala tedy řidiče, aby vystoupil z vozidla a zodpověděl na pár otázek. Jakmile řidič auta vystoupil, začal utíkat, nebylo mu to však platné, policie ho téměř okamžitě zadržela. Policie později našla v jeho autě výbušniny a časovací zařízení.

Nervozita a pocení, kterého si policistka všimla, bylo typickou reakcí limbického mozku na nadměrný stres. Jak již bylo řečeno výše, limbický mozek se nedá obelstít. Řidič se určitě snažil nedat najevo, že v autě veze výbušniny. Díky veliké nervozitě a faktu, že vezl nelegální výbušniny, byl způsoben nátlak na limbický systém, jehož reakcí bylo nadměrné pocení a třas rukou. Jedná se o jeden z prvních případů, kde policista jednal na základě neverbální komunikace. [18]

„*Další důležitou součástí našeho mozku je neokortex, což doslova znamená nová mozková kůra. Této části mozku se také říká "lidský", "myslící" nebo "intelektuální" mozek, protože má na starosti vyšší poznávací činnost a paměť. Právě tato část mozku nás odlišuje od ostatních savců kvůli velkému množství jeho hmoty (kůry) používané k myšlení. Pro jeho schopnost počítat, analyzovat, interpretovat a chápat na úrovni, která je jedinečná pro lidský druh, je to náš kritický a tvůrčí mozek. Je to ale také část mozku, která je nejméně poctivá, a proto je to také náš "prolhaný mozek". Vzhledem k tomu, že je schopen komplexního uvažování, je tento mozek - na rozdíl od svého limbického protějšku - ze všech tří hlavních součástí mozku nejméně spolehlivý. Je to mozek, který umí podvádět a který podvádí často.*“ [18]

Samozřejmě nastává otázka, zda se tyto prvky dají nějakým způsobem skrýt nebo úplně schovat. Odpověď není jednoznačná – ano i ne. Limbický systém jako takový nemůžeme vědomě ovládat, můžeme se však naučit, jak se v určitých případech chovat. Nejprve musíme zjistit, jak se naše tělo chová nebo jakou má náš limbický systém odezvu v různých situacích. Tyto fyzické odezvy následně můžeme zmírnit, ne však úplně vymýtit. Vždycky tam ta tendence k fyzické odezvě bude.

2.2 Projevy neverbální komunikace

Jak již bylo zmíněno výše, neverbální komunikace se může projevovat různými fyzickými odezvami, které se dají velmi často špatně skrýt. V této podkapitole se budeme věnovat tomu, jaké tyto fyzické odezvy mohou mít podobu. Vezmeme si všechny druhy neverbální komunikace postupně, aby bylo vidět, proč jsou důležité a do jaké míry mohou ovlivnit člověka.

2.2.1 Haptika

Haptika je komunikace dotykem. Používá se v celé řadě případů. Dotek je často intimní a může být použit jako akt nadvlády nebo přátelství, záleží na kontextu situace, ve které se člověk nachází.

Jak bylo zmíněno výše, dotekem můžeme nejenom naznačit přátelství, ale také nadvládu nad člověkem. V průmyslu komerční bezpečnosti je tato technika v praxi hojně používána různými bezpečnostními firmami například na nějaké akci. Pokud nastane problém, například, že člověk přijde do objektu, kde nemá co dělat. Pracovník bezpečnostní firmy se ho jednoduše dotkne na rameni, ukáže mu směr a pošle ho tak, kam má jít.

2.2.2 Kinezika

Kinezika neboli také v běžné řeči používaný výraz "řeč těla". To, jak se pohybujeme, jaká gesta používáme při mluveném projevu, všechno spadá pod kineziku. Musíme také rozlišovat různé druhy interpretace. Tyto druhy interpretace řeči těla se mohou lišit na základě kultury nebo pohlaví. Ekman a Friesen vymysleli pět základních účelů, při kterých interpretujeme neverbální komunikaci potažmo kineziku. [19]

2.2.2.1 Znaky

Znaky jsou neverbální signály, které mohou být obecně přeloženy jako slova. Například zdvižený palec může znamenat souhlas. Nebo také typický příklad A-OK, dělá se to pomocí palce a ukazováčku a symbolizuje to OK nebo souhlas. Nicméně, jak již bylo výše uvedeno, v každé kultuře mohou, tyto pro nás typické znaky, být považovány za vulgarismy nebo mohou mít úplně jiný význam.

Obr. 5. A-OK [20]

Například znak OK, který se u nás překládá jako souhlas, znamená v západních kulturách nulu nebo také žádný. V některých kulturách se to dokonce považuje za vulgární gesto, které představuje lidský otvor.

2.2.2.2 Ilustrátory

Ilustrátory jsou pohyby, které doplňují neverbální komunikaci. Lidé používají ilustrátory pro indikaci velikosti objektu nebo také k tomu, aby zdůraznili klíčové slovo ve svém projevu. Ilustrátory napomáhají k tomu, aby se člověk mohl lépe vyjádřit. Je dokázané, že lidem se mluví mnohem lépe, když používají například své ruce k tomu, aby mohly doprovázet proslov nebo aby napomohly k tomu, aby člověk vyjádřil, co potřebuje.

Obr. 6. Ruce v pěst [21]

Čestnost ilustrátorů se může lišit v závislosti na kultuře. Můžeme si jako příklad uvést Italy, kteří jsou typičtí tím, že používají hodně ilustrátorů.

Použití ilustrátorů může pomoci naznačit zájem nebo snahu například o pozornost při zmiňovaném projevu. Na druhou stranu se tyto ilustrátory dají jednoduše přečíst. Stačí si jich všímat, existují typické znaky, které většinou člověk neovlivní. Pokud se bavíme s člověkem, kterého neznáme, a má ruce v pěst, nevěstí to nic dobrého. Je to typický znak toho, že je člověk připraven se bránit nebo dokonce zaútočit. Většinou bychom měli s takovými lidmi jednat s rozvahou. Dalším typickým příkladem mohou být překřížené ruce, což znamená, že nemáme zájem přijímat informace nebo že nesouhlasíme.

2.2.2.3 Projevy emocí

Projevy emocí jsou neverbální projevy těla nebo také obličeje, které nesou emocionální význam. Mohou také naznačit rozpoložení, v jakém se právě nacházíme. Například když vidíme někoho, kdo při chůzi vyskočí, značí to, že člověk je z něčeho šťastný. Naopak člověk, který se pomalu plíží, má svislá ramena a hlavu dolů, je naopak člověk, který je z něčeho nešťastný.

Pokud se zaměříme na projevy emocí v obličeji, můžeme uvést jako příklad člověka, který je zamračený, koutky úst jsou směrem dolů a obočí je také směrem dolů. Tento člověk je ve většině případů v depresi. Nebo typicky člověk, který se usmívá, je většinou šťastný.

Projevy emocí jsou často spontánní a nemůžeme je nijak ovlivnit. Projevy emocí se budu zabývat v další podkapitole, kde budou shrnuty podle Paula Ekmana.

Obr. 7. Deprese [22]

2.2.2.4 Regulátory

Regulátory jsou neverbální zprávy, které doprovázejí řeč. Řídí, regulují nebo napomáhají tomu, co člověk říká. Jako příklad si můžeme uvést řečníka, který když dokončí projev, svěsí obvykle ruce dolů jako gesto ukončení projevu. Může také za pomocí ruky předat slovo kolegovi, který stojí vedle něj. Jako regulátory můžeme také chápat vztyčený prst, jehož význam je stop nebo zastavení.

2.2.2.5 Adaptory

Adaptory jsou formy neverbální komunikace, které se vyskytují na nižší úrovni lidského vnímání. Jinými slovy většina lidí si v daný moment ani neuvědomí, že daný úkon opakuje například neustále dokola. Typickými adaptory je hraní si s vlasy, neustálé cvakání propiskou nebo škrábání, či poopravování brýlí. Jelikož si lidé většinou neuvědomují, že tyto úkony provádí a provádí je s velkou frekvencí, snadno se tak z pohledu pozorovatele dá určit, jak se osoba v dané chvíli cítí, jelikož nám adaptory napovídají.

Obr. 8. Stud, provinilost [23]

Například pokud má člověk pocit provinilosti nebo smutku, tak si zakrývá rukama oči nebo sklopí hlavu dolů a položí ruce na hlavu. Nebo typicky, pokud nás něco bolí, obvykle přiložíme ruku na raněné místo.

2.3 Emoce

Emoce jsou také často nazývány jako pocity. Zahrnují zkušenosti, které jsou spojené s láskou, nenávistí, zlostí, důvěrou, radostí, panikou, strachem nebo smutkem. Emoce se také pojí s náladou, jsou však mírně odlišné. Emoce jsou konkrétní reakce na určité události a mají poměrně krátké trvání. Nálada je spíše obecnější pocit, jako je radost, smutek, frustrace, spokojenost nebo úzkost, které trvají delší dobu.

I když každý prožívá emoce, ne všichni vědci se shodují na tom, co vlastně emoce jsou nebo jak by měly být měřeny nebo studovány. Emoce jsou složité a mají fyzické i psychické prvky. Na čem se však všichni vědci shodují, že součástí emocí jsou subjektivní pocity, fyziologické reakce. Neboli všechny emoce jsou založeny na subjektivních pocitech, které jsou dále vyjádřeny fyziologickými reakcemi.

Někteří vědci se domnívají, že emoce jsou založeny také na kulturních odlišnostech. Ve vědeckém výzkumu, který provedl Ekman spolu s Friesenem, zjistili, že kmeny, které sídlí v přímořském státě Papua Nová Guinea, vykazují stejné známky projevů emocí jako všichni ostatní. Výzkum byl také založen na tom, že tyto kmeny nemají styk s okolním světem, jak už mediální, tak fyzický. Na základě tohoto výzkumu rozdělili emoce do šesti základních obecných skupin: hněv, znechucení, strach, radost, smutek a překvapení.

2.3.1 Hněv

Hněv nebo také vztek jsou emoce, které nelze tak snadno skrýt nebo je maskovat. Jsou to jedny z nejintenzivnějších emocí, které lidé dokážou projevit. Pocity hněvu mohou být zapříčiněny mnoha různými faktory jako třeba, když člověk cítí nespravedlnost, když člověk nesouhlasí s názorem někoho jiného nebo můžou mít také kořeny v našich pudech, člověk se také může rozzuřit, když se cítí v nebezpečí.

Je důležité, abychom byli schopni rozpoznat hněv. Je to důležité proto, protože pokud je člověk rozzuřený, je více náchylný k tomu, aby jednal nerozvážně, ba dokonce ublížil. Bezpečnostní služby, které poskytují ochranu pomocí bodyguardů, trénují tyto lidi, aby byli schopni rozpoznat projevy základních emocí u člověka. Mezi nejdůležitější emoce, které se bodyguardi musejí naučit rozpoznat, je právě hněv. Když si uvedeme příklad, kde bodyguard ochraňuje politika, který má zrovna řečnický projev před publikem. V publiku mohou být lidé, kteří sympatizují s politikem, ale i lidé, kteří s ním nesouhlasí, ba naopak díky jeho projevu jsou rozzuření. Bodyguardi musejí těmto lidem věnovat větší pozornost než ostatním lidem právě proto, že představují větší riziko pro jejich klienta.

Hněv může mít nespočet spouštěčů, tyto spouštěče se také u každého člověka mohou lišit. Všichni lidé však mají společný výraz v obličeji. Tyto výrazy se dají jen těžko zakrýt, jelikož, jak již bylo zmíněno výše, vztek je jedna z nesilnějších emocí, které člověk dokáže cítit a dává je najevo. Hněv můžeme také určit jako stupňující se emoci. Mírný hněv má v obličeji tyto typické znaky, které se mohou dále stupňovat:

- Obočí jsou stáhnutá dohromady a směřují dolů
- Oční víčka jsou přimhouřená, jakoby člověk zaostřoval
- Zúžení rtů

Obr. 9. Hněv [24]

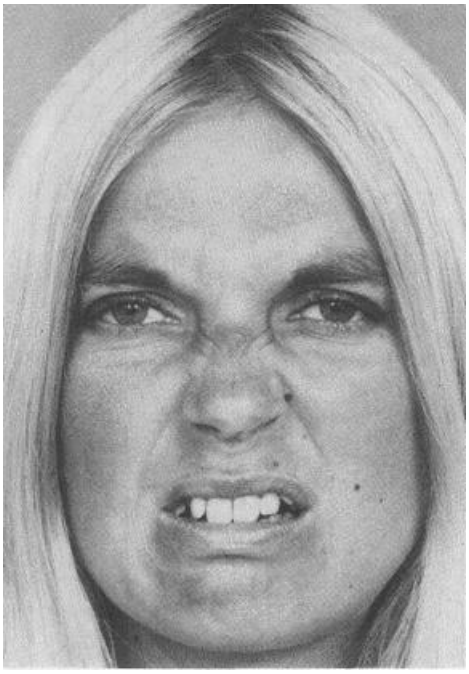
2.3.2 Znechucení

Znechucení je emoce, která může být mířená vůči nějaké osobě ba dokonce i nápadům a názorům dané osoby. Znechucení může být také mířeno vůči nějakému jídlu, které nám nechutná nebo jeví známky hniloby. Obecně se člověk od znechucení distancuje nebo se mu snaží vyhnout. Některé věci, kterými jsme znechuceni, mohou být vrozené, jako například pach z odpadních vod nebo typicky hnijící potraviny.

Znechucení má subjektivní charakter tzn., že každý člověk může mít pocit znechucení z odlišných věcí nebo může cítit znechucení vůči odlišným osobám.

Jak již bylo zmíněno, lidé mohou cítit znechucení vůči ostatním lidem, může to zapříčinit rasový podtext nebo nesouhlas s názorem druhého člověka. Nesouhlas se sice může pojit i se vztekem, ale nesouhlas nemusí přejít ke vzteku, ale k znechucení.

Stejně jako hněv i znechucení má své stupně v závislosti na tom, jak moc je člověk znechucený. Prvky mírného znechucení a silného znechucení se sice liší, význam však zůstává stále stejný. Znechucení ale obecně patří mezi mírné emoční projevy například ve srovnání s hněvem. Nejdůležitější záchytné body k tomu, abychom mohli efektivně rozeznat znechucení, jsou ústa a nos, v menší míře i oční víčka a obočí. Znechucení se projevuje zvednutým horním rtem, spodní ret může být také zvednutý nebo jen povystrčený. Na nose se objeví vrásky. Spodní víčka jsou tlačena nahoru a obočí je snížené.



Obr. 10. Znechucení [24]

2.3.3 Strach

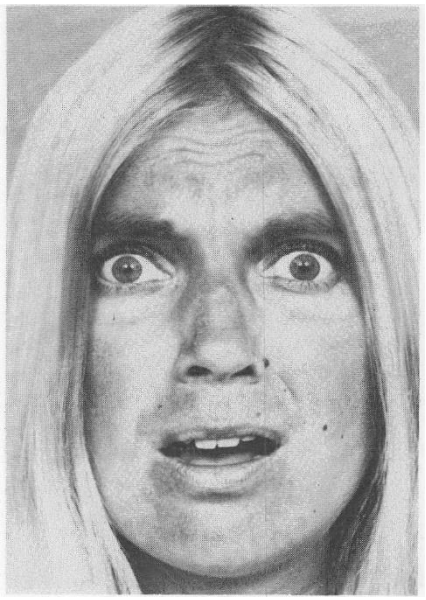
Lidé se bojí ublížení. Škody mohou být jak fyzické, tak i psychické. Fyzické ublížení může být od něčeho menšího, jako jsou třeba mírné odřeniny, nebo až k životu ohrožujícím zraněním. Psychologická újma se může rovněž lišit od menších urážek nebo zklamání až po extrémní útoky na něčí blaho, odmítnutí opětované lásky nebo útok na něčí hodnoty. Lidé se mohou bát všeho, co pro ně představuje nebezpečí, například se mohou bát lidí, zvířat, věcí nebo dokonce i nápadů. Například pokud je člověku řečeno, že příští týden podstoupí řadu bolestivých zákroků, bude pravděpodobně cítit strach, který se bude stupňovat s blížícím se zákrokem.

Strach se stejně jako předchozí emoce může lišit ve své intenzitě. Jak intenzivní může strach být, závisí na předešlých zkušenostech nebo na zhodnocení dané situace.

Strach se často plete s překvapením, avšak strach a překvapení jsou dvě naprosto odlišné emoce. Strach a překvapení se od sebe liší emocionálním stavem, který je doprovázen typickými fyziologickými příznaky. Pokud se člověk cítí v nebezpečí a má strach, jeho kůže může zblednout, srdce tluče rychleji, klepou se ruce, zrychlí se tep, frekvence dýchání, v extrémních případech může dojít až k bolesti žaludku, závratím a zvracení. Tyto pocity trvají z pravidla déle než u překvapení. Například pokud se člověk bojí letět letadlem, může pociťovat

některé tyto příznaky po celou dobu letu. Překvapení trvá krátkou dobu, tedy dobu, než mozek vyhodnotí situaci a nepřiřadí příslušnou reakci. Po překvapení může následovat strach, pocit radosti nebo i smutku.

Při projevu strachu jsou z pravidla obočí zvednutá a stažená k sobě, oči jsou otevřené a víčka napjatá. Na čele se mohou udělat vrásky a nos je mírně sevřený. Horní víčko je mírně zvednuté a spodní víčko je napjaté. Ústa jsou při strachu otevřená a rty jsou napjaté.



Obr. 11. Strach [24]

2.3.4 Radost

Pocit radosti je spjatý s prožíváním příjemných událostí. Radost patří mezi pozitivní emoce. Radost je jednou z nejzákladnějších emocí a dá se snadno přečíst. Stejně jako ostatní emoce i radost se stupňuje a může nabývat na intenzitě. Radost je téměř ve všech případech doprovázena mírným úsměvem na tváři, který podle intenzity může přejít až k posunutí koutků nahoru do maximální možné polohy a v některých případech mohou téct slzy z očí.

Radost je jednou z nejzákladnějších emocí, je však nejvíce používána k tomu, aby maskovala jinou emoci. Proto, ačkoli jde radost nejjednodušeji ztvárnit, si musíme dávat pozor na maskování jiné emoce. Stačí se v podstatě jenom usmát. Radost se také často kombinuje s jinými emocemi, nejčastěji s překvapením. Tato kombinace je typická výrazem úsměvu, zdviženým obočím a vypoulenýma očima. Například když vejde do místnosti přítel, kterého jsme neviděli pět let, tak jsme zároveň šťastní i překvapení. Dále se nejčastěji radost kombinuje se strachem. Například když jedeme na horské dráze. [24]

Obr. 12. Radost [24]

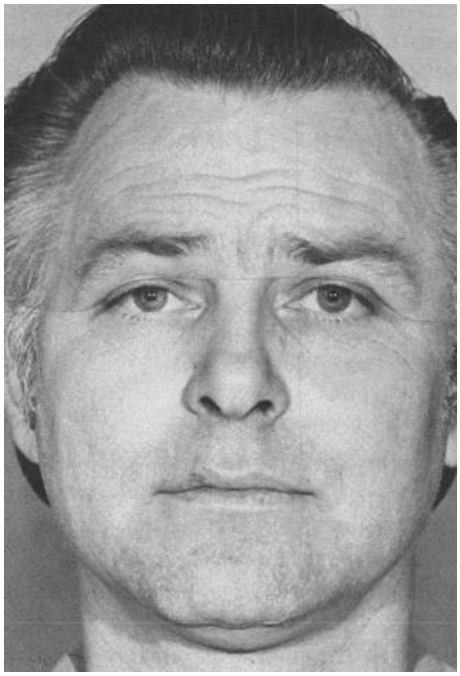
Obr. 13. Kombinace radosti a překvapení [24]

2.3.5 Smutek

Smutek je zapříčiněný nějakým předešlým utrpením. Cokoli může učinit člověka nešťastným nebo smutným. Nejčastěji je však smutek spojován se ztrátou blízkých nebo neopětováním lásky. Může to také být promrhání nějaké životní šance. Smutek je stejně jako strach dlouhodobá emoce na rozdíl třeba od překvapení.

Smutek se dá také vyjádřit jako forma úzkosti, která je nejobecnější a zároveň negativní emoce. Smutek může být v tiché formě nebo hlasité formě (například pláč). Smutek většinou doprovází demotivace nebo výčitky. Nejčastěji se smutek kombinuje se vztekem a strachem. Například smrt blízkého může vyvolat vztek stejně jako úzkost a smutek.

Smutek rozpoznáme jednodušeji v hlasité podobě, protože je doprovázen pláčem. V tiché formě je smutek rozpoznatelný tak, že vnitřní rohy obočí jsou zdvižené a stažené k sobě. Vnitřní koutky horních víček jsou zvednuté, dolní víčko může být také zvednuté. Mohou se také objevit vrásky na čele a mezi obočím. Při silném smutku spadnou koutky pusy dolů.

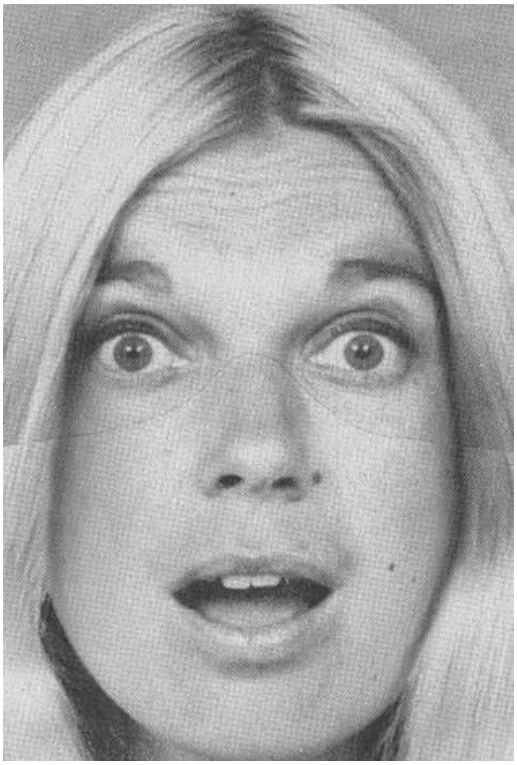


Obr. 14. Smutek [24]

2.3.6 Překvapení

Překvapení je nejkratší emoce, je náhlá jak ve svém nástupu, tak i při odezvě. Pokud má člověk čas na to, aby posoudil, jestli je nebo není překvapený, pak překvapený není. Právě kvůli tomuto důvodu se překvapením dá velice těžko oklamat. Pokud člověk hraje dlouho překvapeného, tak u většiny případů překvapený vůbec není. Opravdové překvapení má stejně rychlou odezvu jako její nástup. Většina lidí, kteří předstírají překvapení, si však neuvědomují, že dělají chybu právě při odezvě překvapení – trvá moc dlouho.

Téměř všechno může být překvapující za předpokladu, že je to neočekávané. Krajina, zvuk, chuť, dotyk nebo vůně může být překvapivé. Překvapivá může být i reakce na nějakou zprávu. Jelikož má překvapení krátké trvání a souvisí s tím, že člověk, který je překvapený, většinou nečekal danou událost nebo informaci, většinou po reakci překvapení nastupují další emoce. Například po překvapení může nastoupit smutek, když nám někdo oznámí špatnou zprávu, nebo může po překvapení nastoupit radost, když nám někdo naopak sdělí radostnou zprávu.



Obr. 15. Překvapení [24]

Stejně jako u ostatních emocí i překvapení se může dostavit v různě intenzivních výrazech, avšak typickým výrazem překvapení jsou formující se vrásky na čele, vypouklé oči a čelist je tlačena směrem dolů. Obočí je mírně zdvižené. V intenzivnějších případech překvapení se přidá úplně zdvižené obočí a otevřená pusa. Výraz překvapení je hodně podobný výrazu strachu, liší se však v tom, že rty nejsou napjaté a nos není sevřený. Jak již bylo zmíněno výše, překvapení se dále kombinuje s ostatními emocemi, které nastupují vzápětí po výrazu překvapení, proto je složitější odhalit právě překvapení, než přijdou na řadu ostatní emoce.

V této kapitole jsme se dozvěděli, co to vlastně neverbální komunikace je a jakým způsobem vlastně funguje. Důležité jsou projevy neverbální komunikace, podle kterých dokážeme zjistit, o jaký druh neverbální komunikace se jedná. Důležitým prvkem toho, abychom mohli rozpoznat projevy neverbální komunikace, jsou emoce. Každá emoce má svůj specifický výraz. Včasnou analýzou těchto výrazů (například znechucení nebo hněvu) v průmyslu komerční bezpečnosti se dá předejít případům, kde může jít o život. Rozpoznání neverbální komunikace a jejím významem nejen v průmyslu komerční bezpečnosti se budeme zabývat v další kapitole.

3 VYUŽITÍ SOCIÁLNÍHO INŽENÝRSTVÍ V PRŮMYSLU KOMERČNÍ BEZPEČNOSTI

Sociální inženýrství jako takové má velké pole působnosti nejen v průmyslu komerční bezpečnosti. V sociálním inženýrství se hodně využívá neverbální komunikace ve všech jejích podobách. Pokud si vezmeme třeba státní správu – tedy konkrétně policii, neverbální komunikace a prvky sociálního inženýrství se zde používají převážně u výslechů. Nemusejí to být ale jen výslechy, mohou to být třeba i policejní vyjednavači, kteří musejí ovládat neverbální komunikaci k tomu, aby dokázali přečíst například člověka, který se zrovna chystá skočit z římsy, a uzpůsobit tomu konverzaci. Cílem je vlastně přesvědčit ho, aby to neudělal.

V průmyslu komerční bezpečnosti můžeme prvky sociálního inženýrství využít například v oblasti bodyguardingu nebo při detekci podezřelého chování na letišti, či jako pracovník ostrahy v obchodním domě. Všude tam, kde profese PKB přichází do styku s lidmi. Jak již bylo zmíněno, neverbální komunikaci používá každý, buď vědomě (cíleně), nebo nevědomě. Na základě správné analýzy neverbálního chování můžeme předejít různým událostem. Ať už je to například u pracovníka ostrahy na letišti, který si vytipuje podezřelou osobu a následně s ní naváže kontakt, aby zjistil, zda se opravdu jedná o nebezpečného člověka. Nebo pracovníka ostrahy v nákupním centru, který vlastně také detekuje podezřelé chování a následně tomu uzpůsobí komunikaci s podezřelým. Dále například v bodyguardingu, kde bodyguard chrání klienta nejen fyzicky, ale také se snaží předejít různým událostem, například pokud vidí člověka, který se blíží ke klientovi s výrazem opovržení nebo zlosti, tak buď klienta odvede, nebo toho člověka konfrontuje a snaží se zjistit, jaký je jeho záměr vůči klientovi. Může to být například prostřednictvím nějakého smyšleného příběhu, se kterým bodyguard právě konfrontuje danou osobu, a snaží se zjistit, zda se ten člověk chystá klientovi ublížit atd.

Přímo sociální inženýrství se dá využít například v bodyguardingu tak, že bodyguard může využít technik sociálního inženýrství k tomu, aby zjistil, zda například obchodní partner jeho klienta ho nechce nijak fyzickým způsobem ohrozit. Na druhou stranu může také prověřit svého klienta, zda s ním mluví na rovinu a je důvěryhodný. Může si vytvořit příběh nebo zápletku, kde bude sledovat reakce, neverbální komunikaci. Díky předem vytvořené zápletce tak může směřovat konverzaci směrem, kterým chce bodyguard. Pokud vidí, že konverzace nejde směrem, kterým chce nebo dotyčný nechce odpovědět na otázku, která je pro bodyguarda stěžejní, může bodyguard zkusit otázku formulovat jinak nebo improvizovat s jinou

zápletkou. Nebo například pokud by byl klient napaden a bodyguard pachatele zpacifikoval, může se bodyguard, za pomocí sociálního inženýrství, dozvědět, zda v okolí nejsou další útočníci, kteří by mohli také ohrozit klienta. Bodyguard může také v rámci sociálního inženýrství dezinformovat možného útočníka.

Stejně jako u bodyguardů, mohou využít sociálního inženýrství strážní v obchodě. Pokud zadrží pachatele, mohou zjistit, zda je pachatel sám nebo má komplice. Pokud se jedná o krádež, může pracovník zjistit, zda pachatel má ukradenou věc u sebe. Pokud pachatel ukradenou věc u sebe nemá, může potom strážný zjistit, kam pachatel tuto věc ukryl. Může tak ušetřit práci policii.

Stejně jako se dá využít sociální inženýrství ve prospěch pracovníka PKB, může být sociální inženýrství využito i pachatelem proti pracovníkovi PKB. V první řadě je třeba si uvědomit, co je cílem pachatele v dané situaci. Pracovník PKB by si měl také dobře uvědomovat, jaký je jeho úkol a pravomoc, aby se nestal terčem sociálního inženýrství. Nejde jenom o to, aby si pracovník PKB osvojil znalosti a techniky spojené se sociálním inženýrstvím, měl by mít zároveň povědomí o tom, jak sociální inženýrství funguje, a tak dokázal včas zareagovat na případný pokus o sociální inženýrství ze strany pachatele.

V rámci využití sociálního inženýrství v průmyslu komerční bezpečnosti jsem oslovil pana Martina Baláže, který pracuje u Policie České republiky (dále jen PČR) – Úřad služby kriminální policie a vyšetřování a v současné době je vedoucím týmu TEMPUS, který se zabývá starými neobjasněnými vraždami, aby mi přiblížil, jakým způsobem se sociální inženýrství i neverbální komunikace využívají u výslechů.

3.1 Rozhovor – Martin Baláž

V této podkapitole je uvedena zkrácená verze rozhovoru s Martinem Balážem. Kompletní rozhovor je příloze bakalářské práce.

1) Jsou nějaké kurzy, školení ohledně výslechů v rámci policie?

„V rámci PČR musí každý kriminalista, který je oprávněn vyšetřovat trestné činy, projít kurzem. Je to vlastně operativně pátrací činnost. V tomto kurzu se učí nejen sledování a pronásledování různých osob, monitoring atd., ale učí se vlastně i výslech, tzn., jak se na ten výslech připravit, co je úkolem toho výslechu a vlastně kam ten výslech by měl směřovat. Z toho se potom skládá zkouška, která je součástí dalších kapitol, a na základě toho on dostane „oprávnění“, je to takový nejnižší stupeň, kdy může pracovat u kriminální policie.

Výslech, tam patří, jak zvládnout výslech, jak komunikovat, jak si připravit výslech, kde výslech provádět, v jakých místnostech apod. Je to součástí budoucí náplně kriminalisty. Dále se potom dají udělat samostatné kurzy, jako je výslech, jak zvládat výslechy, to jsou samostatné kurzy. Celkově je to zaměřené na ty výslechy. Jsou potom i další samostatné kurzy, jak vést tyto výslechy s pachateli nejzávažnější trestné činnosti, popřípadě výslechy mládeže, to jsou zase specializované, na každé ty osoby je to zvlášť. Ne to, co platí na mládež, tak platí na vrahy.“

2) Jaký důraz je kladen u výslechů na neverbální komunikaci v závislosti na tom, co pachatel řekne?

„Určitě, tak když ten kriminalista si ten výslech připraví a započne, tak samozřejmě v první řadě nechá toho člověka mluvit, aby řekl sám všechno. Řekne mu, proč tam je, seznámí ho s předmětem toho výslechu a důležité pro toho policistu je, aby tuto osobu nechal mluvit první sám. Potom teprve až mluví sám, klade doplňující otázky, kde se vlastně zaměří na to, co je mu známo o tom případu, jak to vypadalo na místě činu atd. Cílem je vlastně dostat podezřelou osobu do úzkých tak, aby mluvil pravdu nebo aby se k tomu přiznal. Plánuje se, kde ten výslech bude prováděn, jsou na to specializované výslechové místnosti, kde ten člověk sedí a je vyslýchán. Přes sklo ho můžou sledovat další policisté, popřípadě psycholog, psychiatr, nebo další lidé, kteří jsou zúčastnění na tom úkonu. Musí to být místnost, kde se nebude cítit pohodlně, protože pokud je podezřelý z vraždy, musí se cítit spíše takový ohrožený atd., musí si uvědomovat, co se stalo, a že tam není jenom tak, aby si popovídal s policisty. Je opravdu důležité si tyto věci nachystat.

Záznamová technika, kde ten výslech se zaznamenává, s tím souvisí. Třeba analyzátor hlasu, který potom pomůže policii ukázat, jestli je tam nějaké vnitřní chvění, zda se ten člověk cítil ohrožený nebo necítil, to se potom může nějakým způsobem zužitkovat a přenášet a využít dál. Může k té podezřelé osobě přijít policista s nabídkou fyziodetekčního vyšetření, což je tzv. detektor lži a ten vlastně pomáhá u výslechů. Je to založené na tepové frekvenci, na potivosti, na citlivosti kůže atd. Po fyziodetekčním vyšetření se začnou výsledky vyhodnocovat. Potom dostaneme zprávu, kde vidíme, ve kterých otázkách ten člověk lže nebo se cítil ohrožen atd. To už se ale dělá opravdu u těch nejzávažnějších trestných činů.

Každopádně jak jsem říkal, v první řadě se nechává člověk mluvit, řekne se mu, že je tady ve věci té a té, on by měl sám říct, jak je na té věci zúčastněn atd., a pak se snažíme dávat nějaké doplňující otázky. Samozřejmě, pokud si chceme ověřit pravdivost výslechu, to potom hodně záleží na nonverbální komunikaci, kde ten policista sleduje pachatele. Spousta z nich má na to specializované kurzy, které mu pomohou rozpoznat, zda lže nebo nelže, zda tam jsou nějaké znaky úzkosti, zda hledá nějaké zastání nebo nehledá. Takže ano, je to součástí, ne každý policista tuto zkušenost má, hodně s tím pracují třeba policejní vyjednavači, kteří jsou z řad policie, pak dále kriminální služba, zásahovka. Ti, co jsou z řad kriminální policie, toho využívají u výslechů, kdy oni „poznají“, zda ten člověk mluví pravdu nebo ne. Priorita je nechat ho mluvit, sledovat ho, kam se dívá očima, mimiku tváře, mimiku těla, posed a všechny tyto věci se při výslechu zkoumají.“

3) Nahrává se ten výslech na kameru?

„Samozřejmě se to nahrává jak který výslech, není to povinností. U závažnějších věcí, což je třeba smrt, popřípadě nějaká pedofilie na mládeži, mládeže. Tyto výslechy se nahrávají z důvodu toho, že na tu osobu nebyl činěný nějaký nátlak jak už fyzický, nebo psychický.

Potom se může záznam předložit znalci. Znalec na základě toho udělá analýzu. Protože vlastně pokud je člověk pachatelem, nebo pokud my mu prokážeme, že se dopustil vraždy, tak my ho nějakým způsobem vyslechneme, a pak mu sdělíme obvinění z trestného činu, poté má člověk nárok na obhájce a on buď potom vypovídá, nebo nevypovídá ať tak nebo tak, tak je k tomu člověku přibraný znalec, který ho vyšetří. Vyšetřuje jeho osobnost a vyšetřuje jeho osobnostní profil. Další, co vyšetřuje, je specifická věrohodnost jeho výpovědí, k tomu právě může sloužit ten záznam, na který se ten znalec podívá a na základě toho zpracuje znalecký posudek, zda ten člověk mluvil pravdu nebo nemluvil pravdu.“

4) Říká vám něco jméno Paul Ekman?

„Ekman, zrovna teďka jsme o tom měli přednášku, on se zabývá mimikou tváře a vším tady tímto. Ekmanova metoda řeči těla, řeč tváře. Ale toto umí převážně už osoby, které jsou třeba v kurzu krizové komunikace, policejní vyjednavači, kdy se snažíme na základě mimiky atd. poznat tu osobu, která chce spáchat sebevraždu nebo popřípadě osobu, která drží rukojmí. Je tady několik faktorů, na které se díváme, každý může ukázat něco jiného. Ano, znám tuto metodu a využíváme ji v praxi.“

5) Je podle vás neverbální komunikace u výslechů důležitá?

„Je určitě důležitá, protože na základě toho vlastně jak znalci, tak policisté zjistí, zda jsou tam náznaky lhavosti, zda hledá nějaké zastání, zda vinu svaluje na někoho jiného, zda do toho chce zahrnout třetí osobu. Určitě se využívá často.“

6) Odhadněte, jak často pachatelé spolupracují?

„To je hrozně těžko, pachatelé spoluprací, otázkou je spíš, jaké důkazy má ta policie a podle toho se ten pachatel nebo podezřelá osoba chová. Když vidí, že z toho nevyjde dobře, tak se přizná, protože ví, že dneska přiznání je polehčující okolnost. Pokud si je jistý, že proti němu není schopen nikdo mluvit, tak samozřejmě zapírá a nechá si tu věc dokázat, protože z jeho pohledu je možná nejsnadnější v tu chvíli odmítnout vypovědět. Až mu policie sdělí obvinění, až ukáže ty trumfy, co proti němu má, tak teprve potom začne buď spolupracovat, nebo nezačne. Tam záleží, i jakého má advokáta, těch faktorů je tam víc, vesměs spolupracují pachatelé, kteří nejsou tak kriminálně zdatní, kdy třeba způsobil vraždu a ta pramenila z nevyrovnaných vztahů s manželkou. Nejsou to otřelí kriminálnicí. Co se týče otřelých kriminálníků, tak ti většinou spolupracují tehdy, když vidí, že se z toho nedostanou. Ví, že spoluprací si potom jede o trest a o všechno, může to zúročit u soudu, dostane nižší trest, nižší skupinu ve vězení s menší ostrahou atd.“

7) Myslíte si, že analýza neverbální komunikace, prvky sociálního inženýrství jsou důležité pro PKB?

„Na to se policisté připravují, například při modelových situací. Dá se nachystat na spoustu věcí, ale prostě ve finále, i ze strany policejního vyjednavače můžu říct, že jsme byli připraveni na cokoli, že budeme vyjednávat se sebevrahy, s únosci, všechno toto se stalo, ale ve finále je to všechno úplně jinak. Člověk zažívá takový ten adrenalin, zodpovědnost atd.“

8) Setkal jste se se sociálním inženýrstvím

„Toto není až tak pojem pro kriminalistu nebo pro policistu, toto je spíše takový pojem celkový. Třeba u policie se hodně používá krizová komunikace, toto všechno je zaměřeno na naši práci. Potom dále operativní vytěžování, operativní šetření, výslechy, různé kriminalistické verze atd. Minimum tady s tím sociálním inženýrstvím.“

9) Obsahuje manuál prvky soc. inženýrství?

„To se vyučuje hodně v psychologii, ale říkám, je to hodně specifické. Co se týče policie, je to hrozně zaměřené na tu policejní činnost. Každý ten budoucí policista má možnost si zvolit specifické předměty jako kriminalistka, kriminologie, všechno je spíše zaměřené na tu policejní činnost.“

Jak je vidět z rozhovoru, neverbální komunikace se používá u PČR ve více odvětvích. Mají různé kurzy a školení, které jsou přímo zaměřené na výslechy, na to, jak se u výslechů chovat, jak mluvit s pachatelem. Tyto kurzy jsou dostupné pouze pro PČR. U závažnějších trestných činů používají další zařízení k tomu, aby dokázali lépe rozpoznat, zda pachatel lže nebo ne. Jedná se jak už o fyziodetekční zařízení (detektor lži), analyzátor hlasu, nebo dokonce kameru. Z kamerového záznamu poté dělají analýzu neverbální komunikace, která může dopomoct k usvědčení pachatele. Zajímavostí je také využití tzv. Ekmanovy metody, která je hojně rozšířená v Americe.

Jak je vidět, u policie je pojem neverbální komunikace velmi dobře zavedený, co se týče různých školení atd. Podle mě je tohle důležité i v průmyslu komerční bezpečnosti, daly by se na tom vytvořit kurzy zaměřené na neverbální komunikaci a také na sociální inženýrství, kdyby například tyto kurzy byly dostupné i pro některé zaměstnance v průmyslu komerční bezpečnosti, mohlo by to zásadně pomoct při řešení některých situací. Můžeme například nastínit situaci příslušníka ostrahy na letišti, který eventuálně rozpozná podezřelou osobu, která se nedokáže legitimovat nebo nechce komunikovat. Příslušník ostrahy odvede tuto osobu do místnosti, která je určená k výslechům podobných lidí, kde by mohl uplatnit zkušenosti získané z kurzů týkajících se výslechů, které má k dispozici policie. Detektivové taktéž hojně využívají neverbální komunikaci a sociální inženýrství proto, aby mohli efektivně odvádět svoji profesi. Oproti státní správě nemají detektivové přístup k rozsáhlým databázím, ze kterých by mohli čerpat informace. Musejí si tyto informace dohledat nebo dopátrat sami právě za pomocí sociálního inženýrství.

II. PRAKTICKÁ ČÁST

4 SOCIÁLNÍ EXPERIMENT ZALOŽENÝ NA DOTAZNÍCÍCH

Sociální experiment měl za cíl zjistit, do jaké míry jsou lidé schopni nevědomě prozradit citlivé informace. Sociální experiment se skládá ze dvou dotazníků. Oba dotazníky byly podávány v písemné formě i ve formě elektronické. Jelikož byly výsledky u stěžejních otázek těchto dotazníků u obou forem podobné, byly tyto dotazníky spojeny dohromady. Rozdělené výsledky obou forem dotazníků jsou v příloze bakalářské práce.

První dotazník s názvem Auta z hlediska rozšířenosti byl sestaven pod falešným jménem a fiktivním záměrem. Uvedený záměr dotazníku byl ten, že dotazník má za cíl vypomoct studentovi Vysoké školy Škoda Auto v Mladé Boleslavi, který dotazník potřebuje pro svou bakalářskou práci. Díky zvolenému záměru nevznikl žádný problém ze strany respondentů a všichni, kteří dotazník dostali, jej vyplnili. Otázky byly sestaveny tak, aby nevzniklo žádné podezření a celkově, aby dotazník působil věrohodně. Stěžejní jsou z hlediska bezpečnosti otázky číslo 12, 13 a 14. Ostatní otázky jsou doplňující, které dávají dotazníku celkový dojem důvěryhodnosti. Cílem dotazníku bylo zjistit, kolik informací jsou lidé schopní prozradit o svém autě. Tyto informace by mohly být zneužity zlodějem, který si na základě tohoto dotazníku může vytipovat auto, které by chtěl ukrást.

Druhý dotazník nesl název Zkušenost s dotazníky. Cílem dotazníku bylo zjistit, zda si lidé myslí, že dotazníky mají obecně nějaký přínos, zda lidé odpovídají na dotazníky pravdivě a hlavně, zda by lidé vědomě sdělili soukromé informace prostřednictvím dotazníků. Pro účel dotazníku byly poslední dvě otázky otevřené – lidé museli napsat odpověď ručně. Setkal jsem se s velkou kritikou ze strany respondentů a to, že dotazníky by měly být spíše vyplňovací. Přesto však byly získány uspokojivé informace, které budou dále analyzovány..

4.1 Analýza výsledků prvního dotazníku

1) Jste muž nebo žena?

Tab. 1. Analýza výsledků prvního dotazníku, otázka č. 1

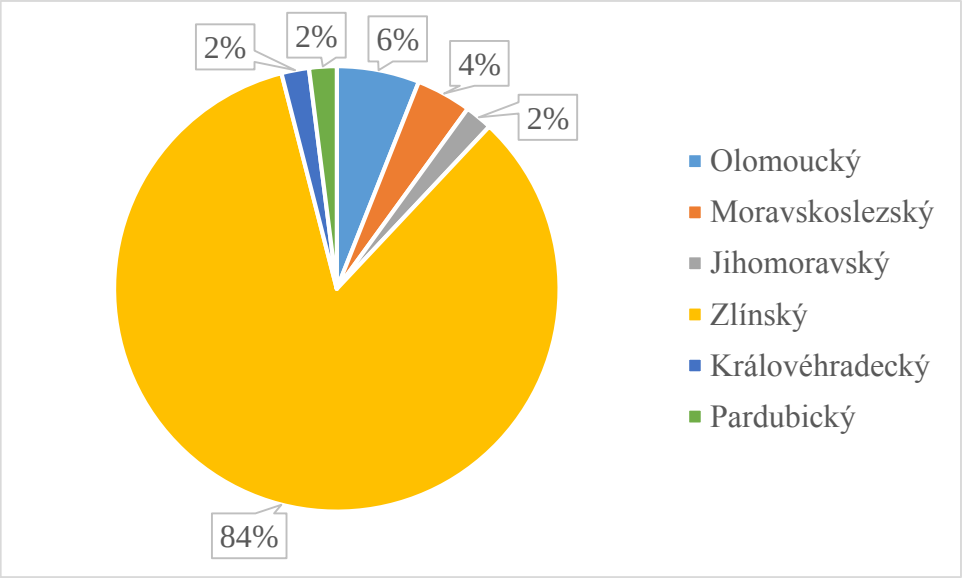
Odpovědi	*Respondenti*	*Podíl*
Muž	36	72%
Žena	14	28%

2) Věk?

Tab. 2. Analýza výsledků prvního dotazníku, otázka č. 2

Odpovědi	*Respondenti*	*Podíl*
18-22	30	60%
23-34	18	36%
35-45	2	4%
46-55	0	0 %
56 a víc	0	0 %

3) Kraj?

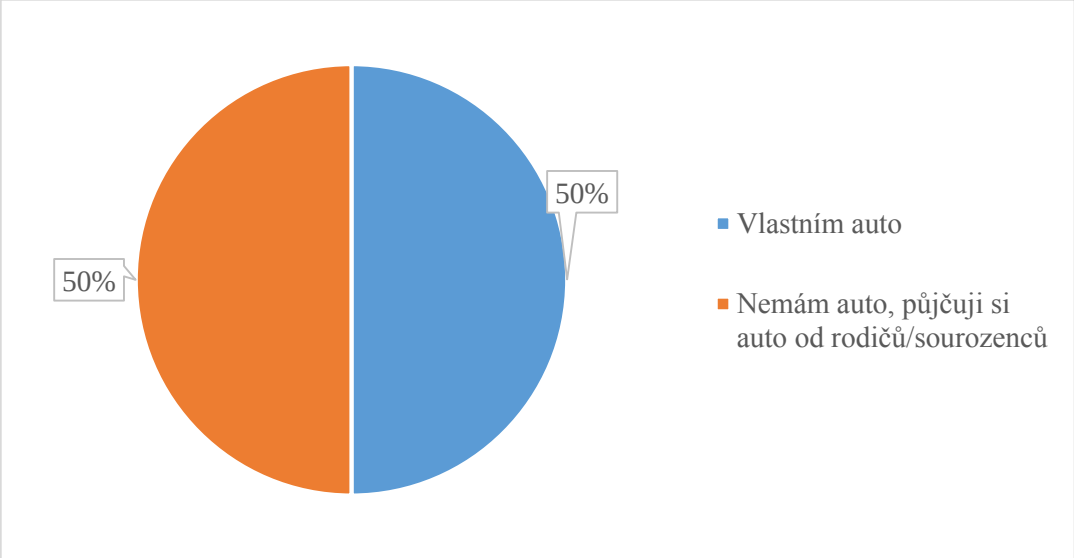


Graf 1. Analýza výsledků prvního dotazníku, otázka č. 3

Tab. 3. Analýza výsledků prvního dotazníku, otázka č. 3

Odpovědi	*Respondenti*	*Podíl*
Hlavní město Praha	0	0 %
Olomoucký	3	6%
Moravskoslezský	2	4%
Jihomoravský	1	2%
Zlínský	42	84%
Kraj Vysočina	0	0 %
Středočeský	0	0 %
Jihočeský	0	0 %
Plzeňský	0	0 %
Karlovarský	0	0 %
Ústecký	0	0 %
Liberecký	0	0 %
Královéhradecký	1	2%
Pardubický	1	2%

4) Vlastníte auto nebo si půjčujete auto někoho jiného?

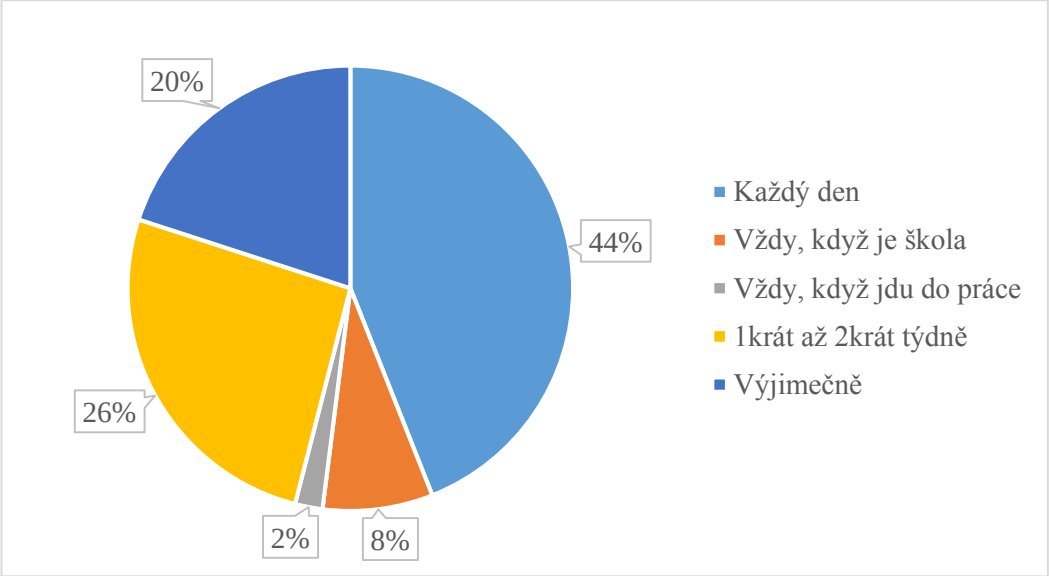


Graf 2. Analýza výsledků prvního dotazníku, otázka č. 4

Tab. 4. Analýza výsledků prvního dotazníku, otázka č. 4

Odpovědi	*Respondenti*	*Podíl*
Vlastním auto	25	40%
Nemám auto, půjčuji si auto od kamaráda	0	0 %
Nemám auto, půjčuji si auto od rodičů/sourozenců	25	50%
Nemám auto, neřídím	0	0%
Sdílím auto s	0	0 %

5) Jak často řídíte?



Graf 3. Analýza výsledků prvního dotazníku, otázka č. 5

Tab. 5. Analýza výsledků prvního dotazníku, otázka č. 5

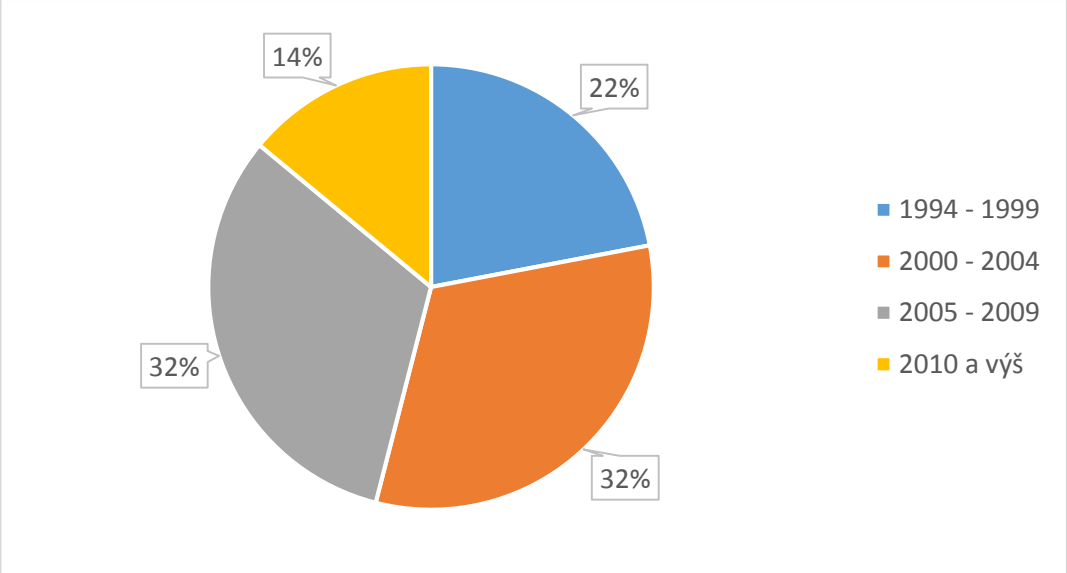
Odpovědi	*Respondenti*	*Podíl*
Každý den	22	47,4 %
Vždy, když je škola	4	21,1 %
Vždy, když jdu do práce	1	5,3 %
1krát až 2krát týdně	13	15,8 %
Výjimečně	10	10,5 %

6) Jaký typ auta řídíte?

Tab. 6. Analýza výsledků prvního dotazníku, otázka č. 6

Odpovědi	*Respondenti*	*Podíl*
Škoda	21	42%
Volkswagen	8	16%
Ford	2	4%
Audi	0	0 %
Opel	2	4%
BMW	3	6%
Renault	5	10%
Fiat	0	0 %
Toyota	2	4%
Jiné	7	14%

7) Rok výroby auta?



Graf 4. Analýza výsledků prvního dotazníku, otázka č. 7

Tab. 7. Analýza výsledků prvního dotazníku, otázka č. 7

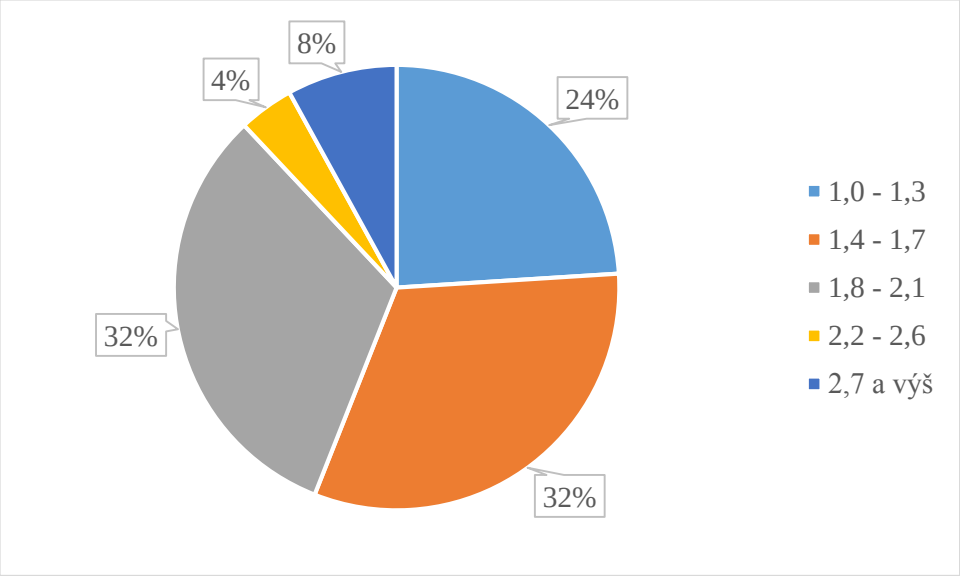
Odpovědi	*Respondenti*	*Podíl*
1994 - 1999	11	22%
2000 - 2004	16	32%
2005 - 2009	16	32%
2010 a výš	7	14%

8) Typ motoru?

Tab. 8. Analýza výsledků prvního dotazníku, otázka č. 8

Odpovědi	*Respondenti*	*Podíl*
Benzín	35	70%
Diesel	15	30%
Kombinace s LPG	0	0 %

9) Obsah motoru? (Hodnoty jsou v litrech)

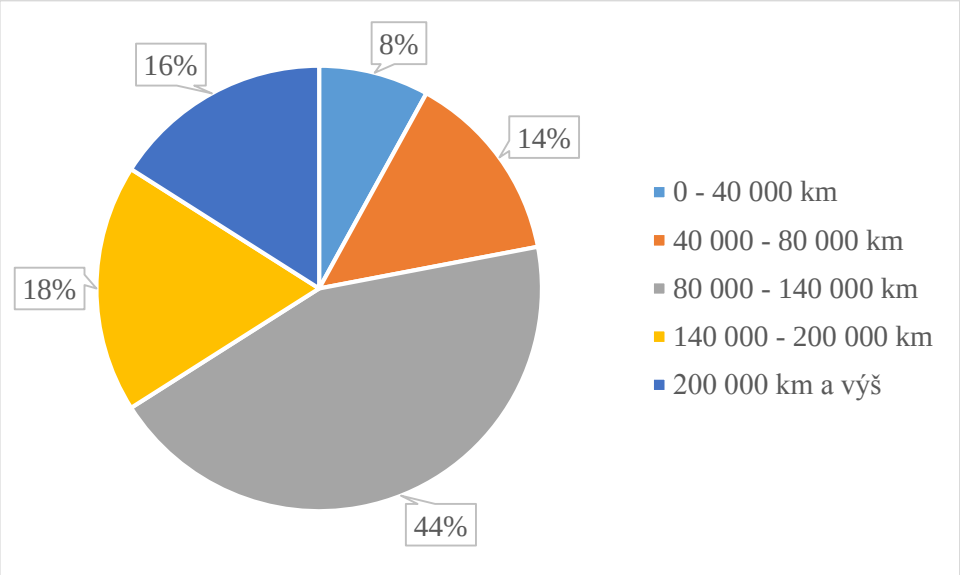


Graf 5. Analýza výsledků prvního dotazníku, otázka č. 9

Tab. 9. Analýza výsledků prvního dotazníku, otázka č. 9

Odpovědi	*Respondenti*	*Podíl*
1,0 - 1,3	12	24%
1,4 - 1,7	16	32%
1,8 - 2,1	16	32%
2,2 - 2,6	2	4%
2,7 a výš	4	8%

10) Najeté kilometry?

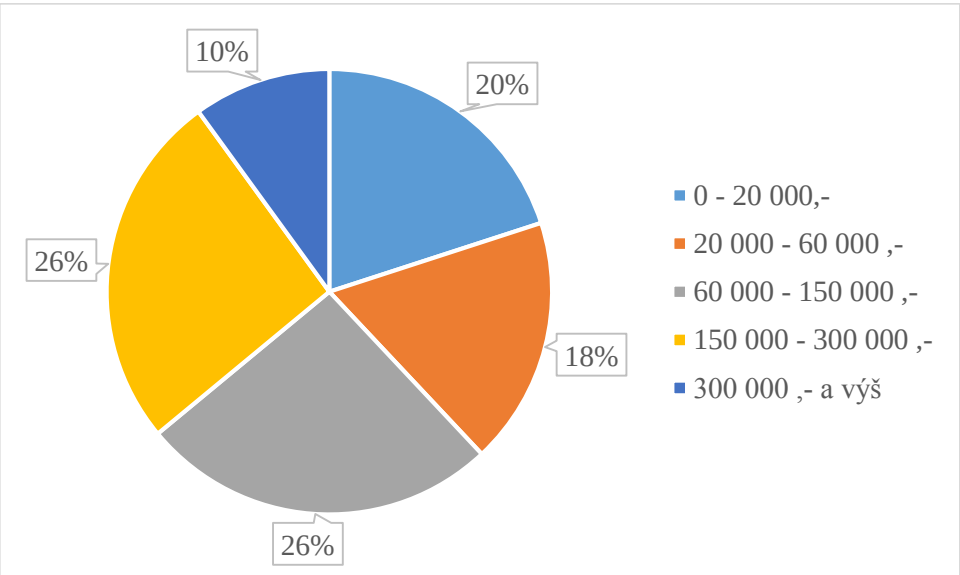


Graf 6. Analýza výsledků prvního dotazníku, otázka č. 10

Tab. 10. Analýza výsledků prvního dotazníku, otázka č. 10

Odpovědi	***Respondenti***	***Podíl***
0 - 40 000 km	4	8%
40 000 - 80 000 km	7	14%
80 000 - 140 000 km	22	44%
140 000 - 200 000 km	9	18%
200 000 km a výš	8	16%

11) Odhadovaná cena auta?

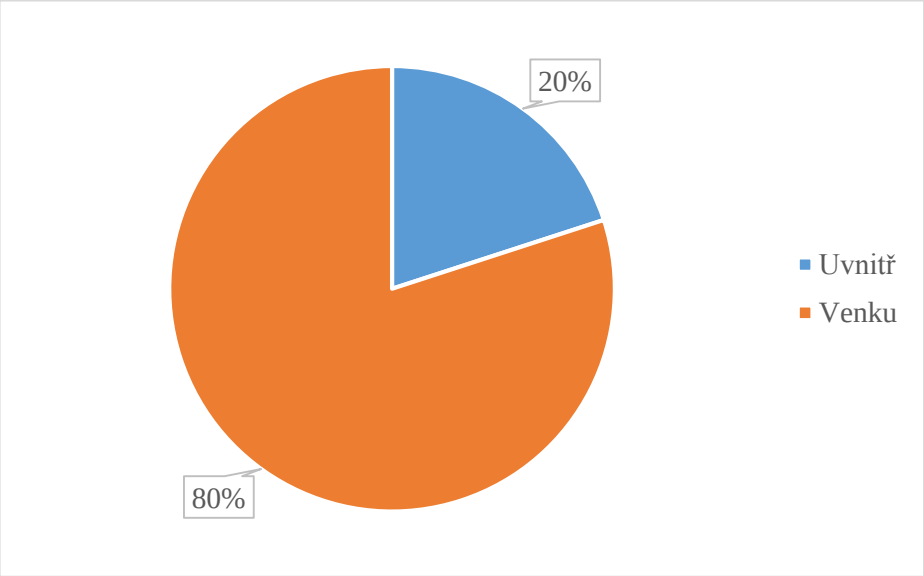


Graf 7. Analýza výsledků prvního dotazníku, otázka č. 11

Tab. 11. Analýza výsledků prvního dotazníku, otázka č. 11

Odpovědi	*Respondenti*	*Podíl*
0 - 20 000,-	10	20%
20 000 - 60 000,-	9	18%
60 000 - 150 000,-	13	26%
150 000 - 300 000,-	13	26%
300 000,- a výš	5	10%

12) Parkujete spíše uvnitř/venku ?

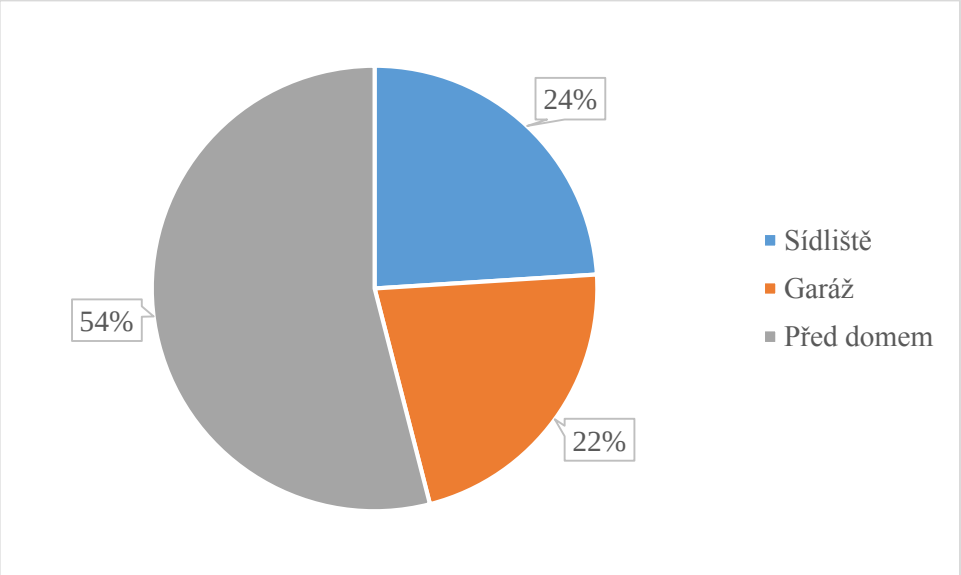


Graf 8. Analýza výsledků prvního dotazníku, otázka č. 12

Tab. 12. Analýza výsledků prvního dotazníku, otázka č. 12

Odpovědi	*Respondenti*	*Podíl*
Uvnitř	10	20%
Venku	40	80%

13) V jaké lokalitě parkujete?

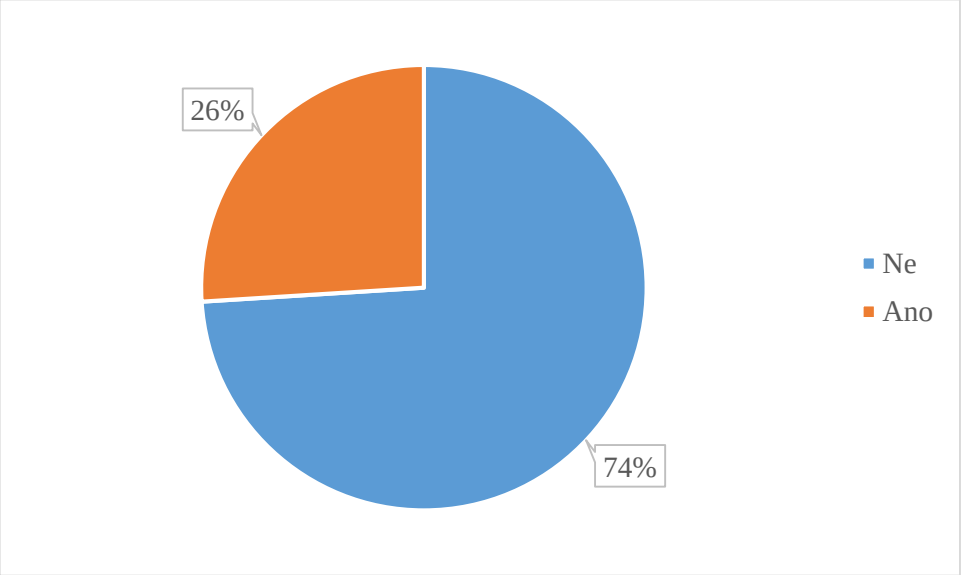


Graf 9. Analýza výsledků prvního dotazníku, otázka č. 13

Tab. 13. Analýza výsledků prvního dotazníku, otázka č. 13

Odpovědi	Respondenti	Podíl
Sídliště	12	24%
Hlídané parkoviště	0	0 %
U obchodního centra	0	0 %
Garáž	11	22%
Před domem	27	54%
Jinde	0	0 %

14) Má dané auto nějaké zabezpečení, které není v základní výbavě auta? Pokud ano, jaké? (Zámek pedálů, volantu, GPS ...)



Graf 10. Analýza výsledků prvního dotazníku, otázka č. 14

Tab. 14. Analýza výsledků prvního dotazníku, otázka č. 14

Odpovědi	Respondenti	Podíl
Ne	37	74 %
Ano	13	26 %

Lidé, kteří odpověděli na tuto otázku Ano, uvedli také, jaké zabezpečení navíc mají. Jednalo se převážně o zámek volantu a zámek řadicí páky (zpátečky).

4.1.1 Dílčí závěr

Jak již bylo výše zmíněno, stěžejní otázky z hlediska bezpečnosti byly otázky číslo 12, 13 a 14. Většina respondentů u tohoto dotazníku odpovídala ve formě písemné, což může být pro potencionálního pachatele ještě mnohem větší výhoda, než vyplněný dotazník v elektronické podobě, protože si může člověka vytipovat, ví, jak vypadá a může ho například sledovat, aby zjistil, kde přesně bydlí.

Výsledkem dotazníku Auta z hlediska rozšířenosti je, že 80% tázaných lidí parkuje venku, což je pro potencionálního pachatele důležité. Snadněji tak může auto odcizit. Ze všech tázaných lidí 54% lidí parkuje před domem a 24% lidí parkuje na sídlišti. Jak již bylo výše zmíněno, pro potencionálního pachatele je tato informace také stěžejní, může si tak vybrat

auto, které se dá snadněji ukrást, například v porovnání s parkujícím autem v garáži (z dotazníků 22%). Poslední stěžejní otázka je taktéž velmi důležitá pro potencionálního pachatele. Bylo zjištěno, že 74% z dotazovaných lidí nemá žádné zabezpečení, které by nebylo v základní výbavě auta. Potencionální pachatel tak u většiny aut nemusí předpokládat větší odpor ze strany auta při odcizování. Na druhou stranu téměř 26% lidí dobrovolně odpovědělo, že v autě je zabezpečení navíc, které není v základní výbavě auta. Lidé dokonce dobrovolně napsali, o jaké zabezpečení se jedná, jsou to převážně zámky řadicí páky a zámky volantů.

Potencionální pachatel, za účelem vytipování osoby, může dotazník podávat v písemné podobě (lze i v elektronické podobě, nesmí však dotazník rozesílat hromadně). Získá tak informace o tom, jaké má dotazovaný auto – značka, obsah motoru, odhadovaná cena, ujeté kilometry. Také zjistí, kde respondent parkuje auto, jestli je auto jeho nebo auto s někým sdílí, zda má auto zabezpečení, pokud ano, tak jaké. Díky tomu se může například pachatel rozhodnout, jaké auto je pro něj jednodušší k odcizení.

4.2 Analýza výsledků druhého dotazníku

1) Jste muž nebo žena?

Tab. 15. Analýza výsledků druhého dotazníku, otázka č. 15

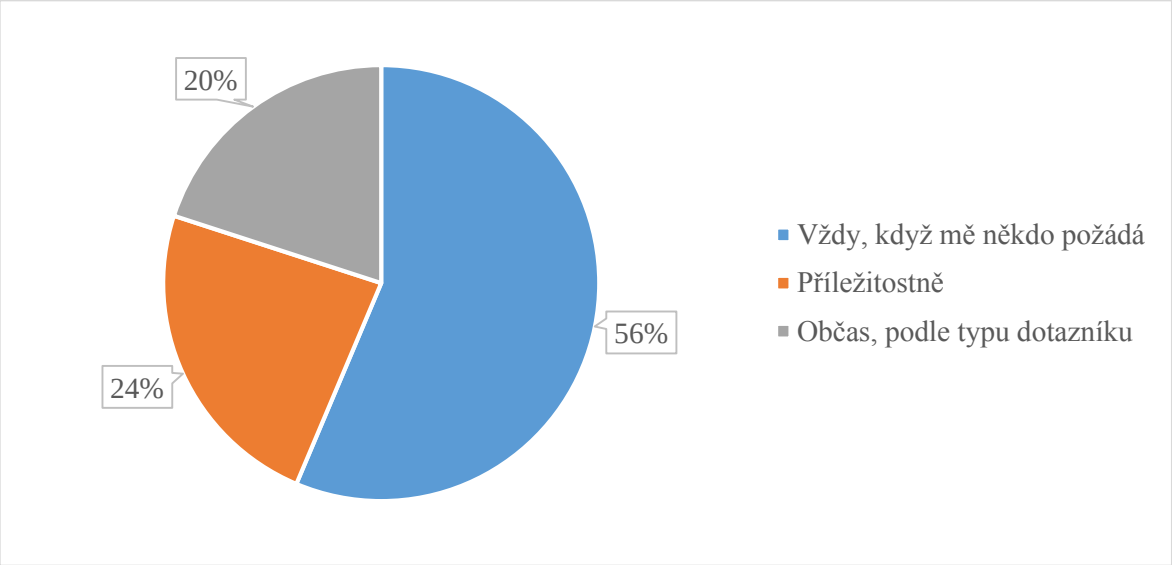
Odpovědi	Respondenti	Podíl
Muž	31	56%
Žena	24	44%

2) Věk?

Tab. 16. Analýza výsledků druhého dotazníku, otázka č. 2

Odpovědi	Respondenti	Podíl
14 - 17	0	0%
18 - 22	32	58%
23 - 34	20	36%
35 - 45	2	4%
46 a víc	1	2%

3) Jak často vyplňujete dotazníky? Zkuste odhadnout, jak často.

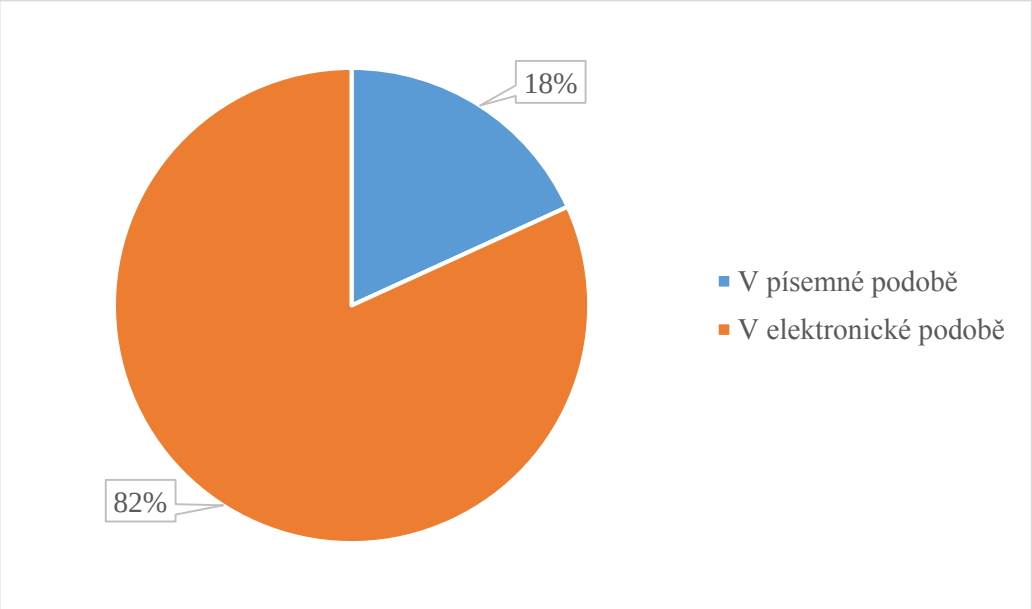


Graf 11. Analýza výsledků druhého dotazníku, otázka č. 3

Tab. 17. Analýza výsledků druhého dotazníku, otázka č. 3

Odpovědi	Respondenti	Podíl
Vždy, když mě někdo požádá	31	56%
Příležitostně	13	24%
Občas, podle typu dotazníku	11	20%

4) V jaké podobě se s dotazníky nejčastěji setkáváte?

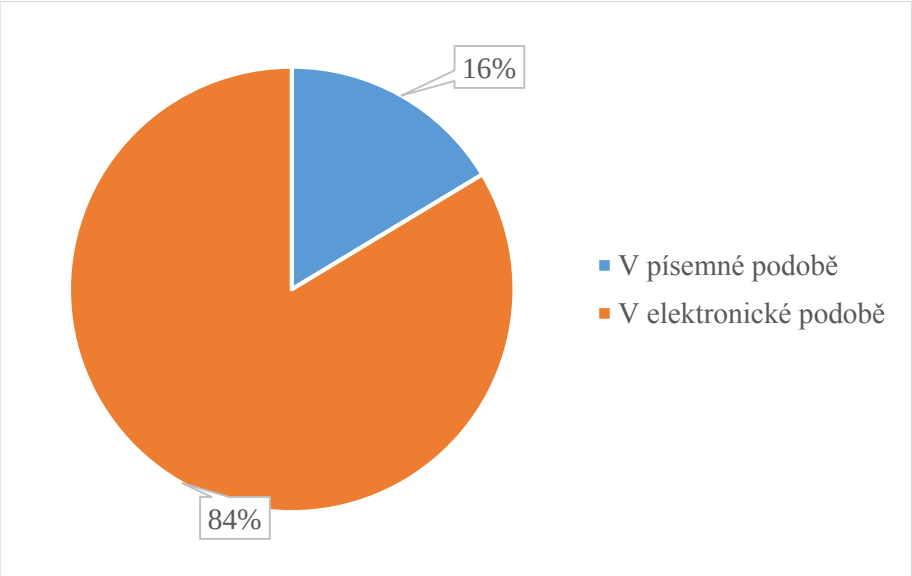


Graf 12. Analýza výsledků druhého dotazníku, otázka č. 4

Tab. 18. Analýza výsledků druhého dotazníku, otázka č. 4

Odpovědi	Respondenti	Podíl
V písemné podobě	10	18%
V elektronické podobě	45	82%
Po telefonu	0	0%

5) Jaká podoba dotazníku je pro vás přijatelnější?

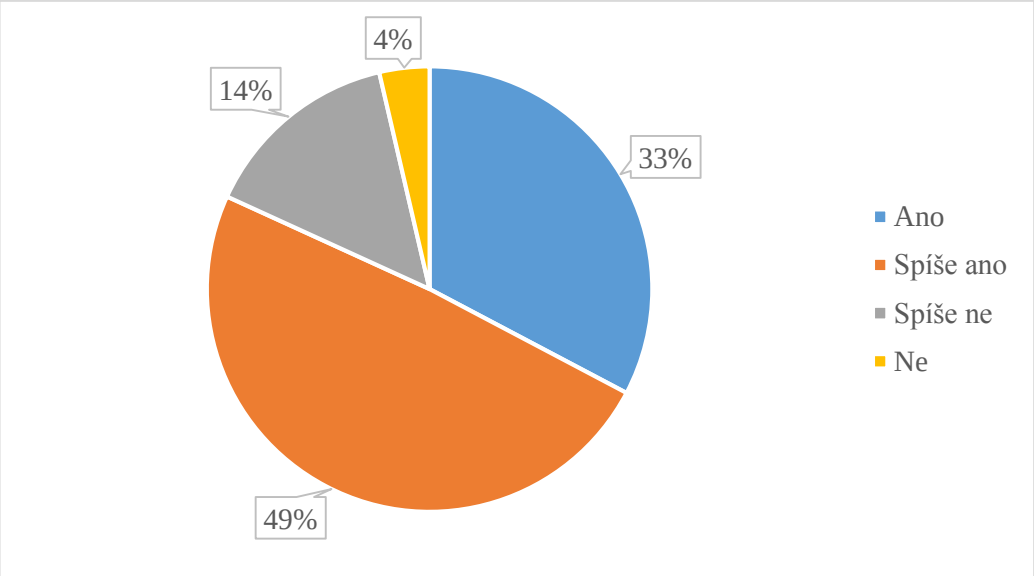


Graf 13. Analýza výsledků druhého dotazníku, otázka č. 5

Tab. 19. Analýza výsledků druhého dotazníku, otázka č. 5

Odpovědi	Respondenti	Podíl
V písemné podobě	9	16%
V elektronické podobě	46	84%
Po telefonu	0	0%

6) Myslíte si, že dotazníky mají obecně nějaký přínos?

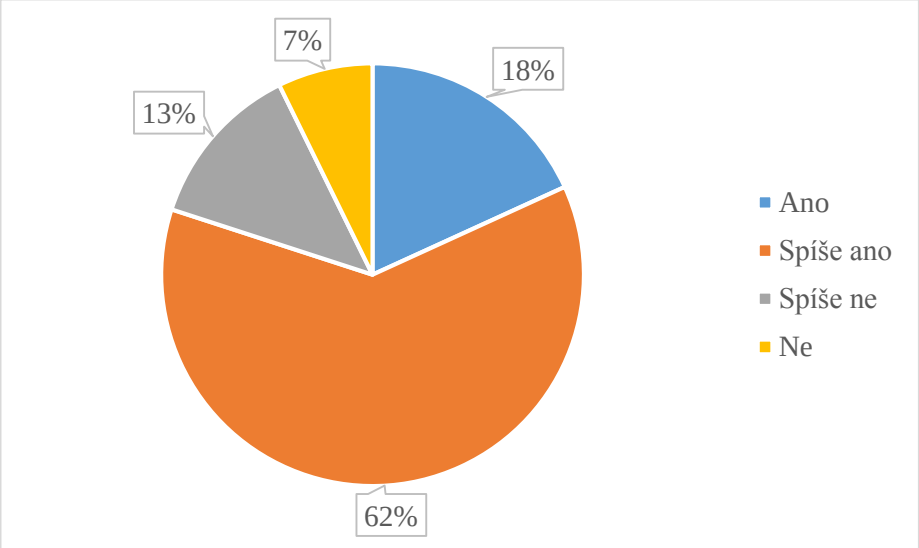


Graf 14. Analýza výsledků druhého dotazníku, otázka č. 6

Tab. 20. Analýza výsledků druhého dotazníku, otázka č. 6

Odpovědi	Respondenti	Podíl
Ano	18	33%
Spíše ano	27	49%
Spíše ne	8	14%
Ne	2	4%

7) Myslíte si, že výstupní hodnoty z dotazníků jsou důvěryhodné a dá se s nimi dál pracovat?

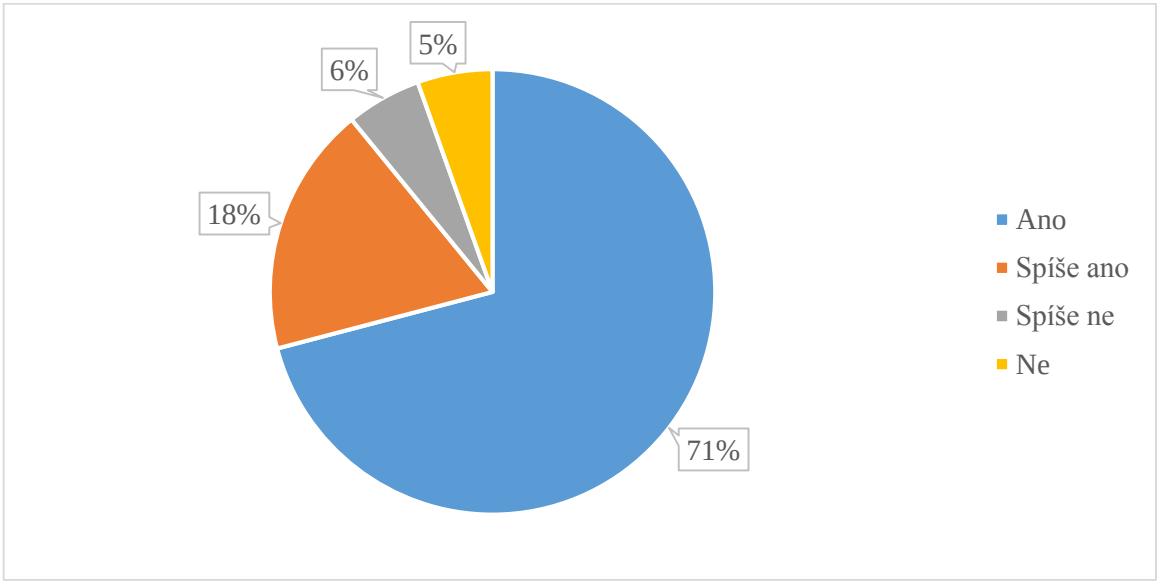


Graf 15. Analýza výsledků druhého dotazníku, otázka č. 7

Tab. 21. Analýza výsledků druhého dotazníku, otázka č. 7

Odpovědi	Respondenti	Podíl
Ano	10	18%
Spíše ano	34	62%
Spíše ne	7	7%
Ne	4	13%

8) Vyplňujete dotazníky pravdivě?

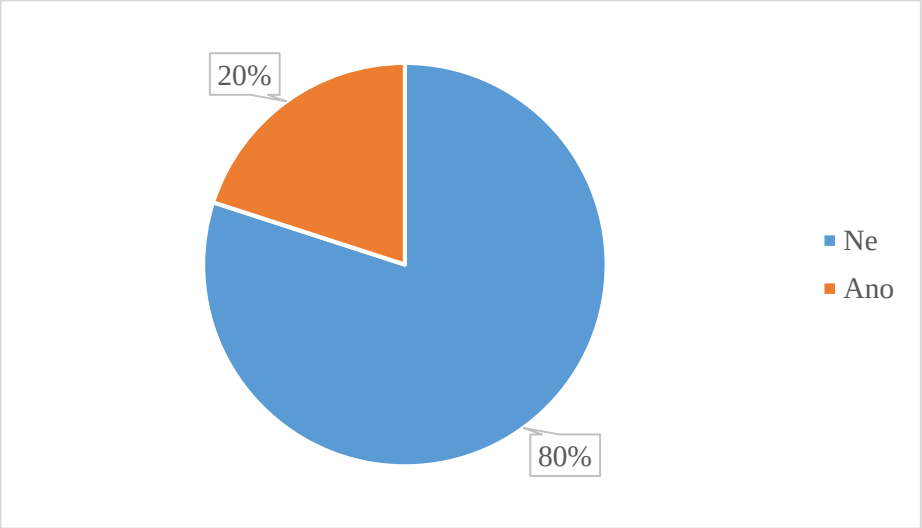


Graf 16. Analýza výsledků druhého dotazníku, otázka č. 8

Tab. 22. Analýza výsledků druhého dotazníku, otázka č. 8

Odpovědi	Respondenti	Podíl
Ano	39	71%
Spíše ano	10	18%
Spíše ne	3	6%
Ne	3	5%

9) Sdělili byste soukromé informace (např. jméno, výdělek, adresu...) v rámci dotazníku? Pokud ano, které?



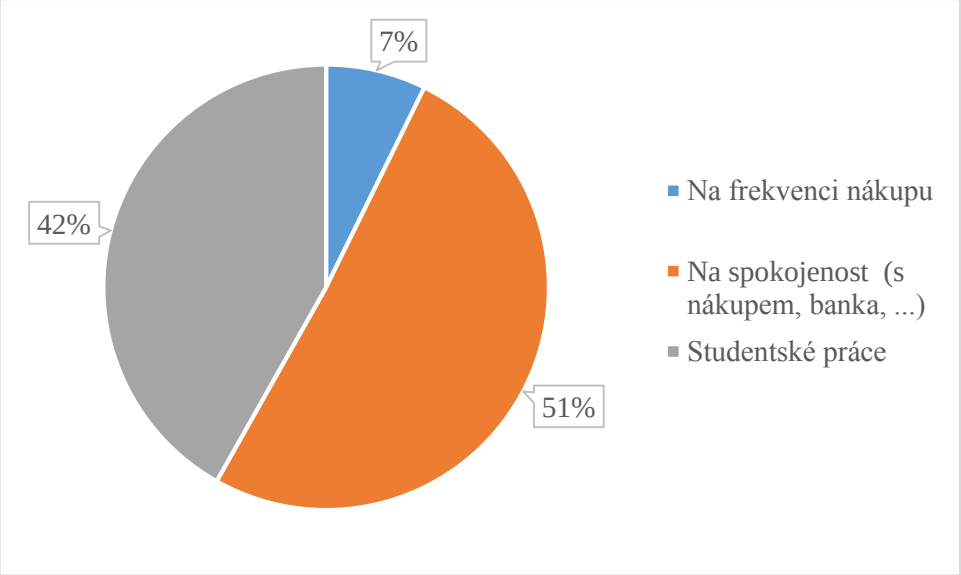
Graf 17. Analýza výsledků druhého dotazníku, otázka č. 9

Tab. 23. Analýza výsledků druhého dotazníku, otázka č. 9

Odpovědi	Respondenti	Podíl
Ne	44	80%
Ano	11	20%

Téměř polovina lidí, kteří u této otázky odpověděli Ano, připisovali, že by prozradili informace jako jméno a výdělek. Druhá polovina lidí odpověděla, že by záleželo na typu dotazníku.

10) Jaké zaměření mají obvykle dotazníky, které vyplňujete?



Graf 18. Analýza výsledků druhého dotazníku, otázka č. 10

Tab. 24. Analýza výsledků druhého dotazníku, otázka č. 10

Odpovědi	Respondenti	Podíl
Na frekvenci nákupu	4	7%
Na spokojenost (s nákupem, banka, ...)	28	51%
Studentské práce	23	42%

11) Napište několik příkladů otázek, se kterými jste se v dotaznících setkali?

Cílem této otázky bylo se dozvědět, jaké typy otázek se používají v dotaznících. Kromě otázek na věk a pohlaví, nejčastější odpovědi byly – Jak často nakupujete, Kolik peněz měsíčně utratíte, Spokojenost s pojišťovnou.

12) S jakou nejzajímavější nebo nejkurióznější otázkou jste se v dotaznících setkali?

Cílem této otázky bylo zjistit, s jakými nejkurióznějšími otázkami se respondenti v dotaznících setkali. Překvapivě nejčastější odpovědí bylo, jaký je váš PIN nebo jak dlouhé heslo používáte.

4.2.1 Dílčí závěr

U tohoto dotazníku již nebylo tak důležité, v jaké formě respondenti dotazník vyplní. Převážná většina lidí odpovídala elektronickou formou. Pro porovnání jsou obě formy dotazníků v příloze bakalářské práce.

Jedním z hlavních cílů dotazníku Zkušenost s dotazníky bylo zjistit, zda lidé odpovídají na dotazníky pravdivě. Z celkového počtu 55 lidí, kteří odpověděli, 71% lidí odpovídá na dotazníky jednoznačně pravdivě a 18% lidí odpovědělo Spíše ano, což se také dá považovat za uspokojivou a výchozí odpověď. Pokud se odkážeme na první dotazník, tak můžeme říci, že téměř většina respondentů odpovídala pravdivě, což je hodně potřebné k tomu, aby byl dotazník brán jako důvěryhodný například pro potencionálního pachatele, jako tomu bylo u prvního dotazníku.

Další důležitou otázkou bylo, zda by lidé sdělili osobní informace prostřednictvím dotazníku. Velká část, tedy 80%, dotazovaných odpovědělo, že by nesdělili soukromé informace prostřednictvím dotazníku. Z toho vyplývá, že záleží na tom, jakým způsobem jsou otázky v dotazníku položeny a za jakým cílem je dotazník vytvořen. Pokud se znovu odkážeme na předchozí dotazník, tak i přesto, že by většina lidí neposkytla soukromé informace prostřednictvím dotazníku, tak všichni lidé, bez jakýchkoli okolků, odpověděli na otázky typu, zda parkují své auto venku nebo uvnitř a jestli má auto nějaké zabezpečení. Jednoduše se tedy dá sestavit cílený dotazník, který vytěžuje soukromé informace, aniž by to člověka napadlo. Spíše naopak, co se týká prvního dotazníku, většina respondentů hned po tom, co jsem řekl, že kamarád potřebuje vyplnit dotazník pro svoji bakalářskou práci, byli rádi, že mi dotazník vyplnili.

Poslední dvě otázky v dotazníku byly otevřené. Přesto, že jsem se setkal s velkou kritikou kvůli tomu, že lidem není pohodlné vyplňování dotazníků slovně, se vrátilo hodně odpovědí. Zajímavé je, že hodně respondentů uvádělo jako nejkurióznější otázku v dotazníku – Jaký je váš PIN nebo jak dlouhé je vaše heslo. Zdá se, že někteří lidé se již snaží pomocí dotazníků využívat ochoty lidí odpovídat na dotazníky a čekají, kdo se nachytá.

Co se týká poslední otázky, zhruba polovina respondentů odpovídá většinou na dotazníky ohledně spokojenosti. 42% lidí potom odpovídá na dotazníky týkajících se studentských prací. První dotazník se tvářil jako dotazník, který měl pomoct studentovi s bakalářskou prací. Lidé, potažmo studenti, tyto dotazníky rádi vyplňují, mají pocit, že tak pomáhají spolužákovi nebo jinému studentovi. Čili je jednoduché, jako to bylo i u prvního dotazníku, dostat z těchto lidí informace, které člověk potřebuje, pod záštitou pomoci.

4.3 Shrnutí obou dotazníků

Oba dotazníky byly rozšířeny jak ve formě elektronické, tak ve formě písemné mezi studenty. U prvního dotazníku – Auta z hlediska rozšířenosti, bylo důležité, aby byl dotazník rozšířen převážně v písemné formě. Jeho cílem bylo zjistit, kolik informací jsou lidé schopní prozradit o svém autě. Tyto informace by mohly být zneužity zlodějem, který si na základě tohoto dotazníku může vytipovat auto, které by chtěl ukrást. Osobním kontaktem s respondentem si může zapamatovat vytipovanou osobu, což může ulehčit pozdější krádež auta. Z dotazníku vyplynulo, že 80% respondentů parkuje auto venku, což může být pro potenciálního pachatele výhoda. Celých 74% z dotazovaných lidí nemá na autě žádné zabezpečení, které není obsažené v továrně vyrobeném autě. Zbylých 26% lidí se přiznalo, že má v autě zabezpečení navíc, dokonce i připsali jaké. Jednalo se převážně o zámky řadicí páky a zámky volantů. Druhý dotazník s názvem Zkušenost s dotazníky měl za cíl zjistit, zda lidé odpovídají na dotazníky pravdivě. Celých 71% lidí odpovědělo, že na dotazníky odpovídá jednoznačně pravdivě, dalších 18% lidí odpovědělo Spíše ano. Dalším důležitým cílem dotazníku bylo zjistit, zda by lidé prostřednictvím dotazníku sdělili soukromé informace. Z celkového počtu lidí 80% lidí odpovědělo, že by nesdělili soukromé informace prostřednictvím dotazníku. Vzhledem k tomu, že v prvním dotazníku byly položeny otázky, týkající se bezpečnosti, které lze považovat za citlivé, můžeme říct, že záleží na tom, jakým způsobem jsou otázky v dotazníku položeny a za jakým cílem je dotazník vytvořen a představen respondentům. Součástí druhého dotazníku byly také otevřené otázky, které měly zjistit, s jakými otázkami se respondenti již při vyplňování dotazníků setkali. Zajímavé je, že hodně respondentů uvádělo jako nejkurióznější otázku v dotazníku – Jaký je váš PIN nebo jak dlouhé je vaše heslo.

ZÁVĚR

V této práci byly vysvětleny základní pojmy, které jsou spojené se sociálním inženýrstvím. Byl zde vysvětlen rozdíl mezi sociálním inženýrstvím, které je obecně bráno jako internetová hrozba, a sociálním inženýrstvím v reálném světě. Byly popsány jednotlivé techniky sociálního inženýrství a jejich využití v praxi. Byl zde vysvětlen pojem neverbální komunikace, který je nedílnou součástí sociálního inženýrství. V bakalářské práci byly vysvětleny základní pojmy, které souvisí s neverbální komunikací. Dále byly uvedeny, jaké jsou základní projevy neverbální komunikace a emoce, které jsou s ní spjaty a díky kterým ji dokážeme přesněji analyzovat. Projevy emocí jsou doprovázeny typickými znaky, které se dají vyčíst z obličeje. Velkou částí také přispěl pan Martin Baláž, který poskytl rozhovor na téma neverbální komunikace a jeho využití u policie. Dozvěděli jsme se, jaké techniky používá policie k tomu, aby odhalila případnou lež u výslechů. Hlavní součástí teoretické části je také využití sociálního inženýrství v průmyslu komerční bezpečnosti. Své uplatnění najde v řadách detektivů, bodyguardů nebo také u ostrahy. Uplatnění může najít téměř ve všech profesích průmyslu komerční bezpečnosti, kde člověk přichází do styku s lidmi.

Přínos teoretické části je zejména v objasnění pojmů spojených se sociálním inženýrstvím a to, že sociální inženýrství není jenom pojem spojený s internetovou kriminalitou, ale že se s tím lidé mohou setkat i v reálném světě. Využití sociálního inženýrství v průmyslu komerční bezpečnosti je možné například detektivy nebo bodyguardy. Dalším přínosem je rozhovor s Martinem Balážem, který pracuje u policie a má letité zkušenosti s výslechem. V rozhovoru je nastíněno, jakým způsobem se policie staví k problematice používání neverbální komunikace u výslechů a jakým způsobem se na výslechy chystají.

V praktické části bakalářské práce byl proveden sociální experiment, který byl založený na dotaznících. Sociální experiment splnil cíl, kterým bylo zjistit, do jaké míry jsou schopni lidé prozradit citlivé informace za pomocí dotazníků. Experiment se skládal ze dvou dotazníků, kde každý hrál svou roli. První dotazník – Auta z hlediska rozšířenosti - byl sestaven tak, aby zjistil citlivé informace ze stran respondentů. Lidé ochotně dotazník vyplňovali a byli rádi, že mohou pomoct fiktivní osobě v její bakalářské práci. Druhý dotazník měl za cíl zjistit, zda lidé odpovídají na dotazníky pravdivě a celkově s jakými zajímavými otázkami se lidé při vyplňování dotazníků setkali.

Přínos praktické části vidím v tom, že dotazníky mohou být zneužity k tomu, aby získaly citlivé informace z řad respondentů. Záleží jenom na pachateli, jakým způsobem sestaví dotazník a mezi jakými lidmi ho bude rozšiřovat. Lidé by si měli uvědomovat, co vyplňují, komu to vyplňují a proč to vyplňují.

SEZNAM POUŽITÉ LITERATURY

[1] What is Social Engineering? In: *WEBROOT* [online]. [cit. 2016-04-09]. Dostupné z: http://www.webroot.com/hk/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering

[2] ROUSE, Margaret. Social engineering. *SearchSecurity* [online]. , 2 [cit. 2016-04-09]. Dostupné z: http://searchsecurity.techtarget.com/definition/social-engineering

[3] GOODCHILD, Joan. Social engineering techniques: 4 ways criminal outsiders get inside. *CSO Online* [online]. , 3 [cit. 2016-04-09]. Dostupné z: http://www.csoonline.com/article/2125205/social-engineering/social-engineering-techniques--4-ways-criminal-outsiders-get-inside.html

[4] WHITAKER, Andrew. Top 10 Social Engineering Tactics. *InformIT* [online]. , 10 [cit. 2016-04-09]. Dostupné z: http://www.informit.com/articles/article.aspx?p=1350956&seqNum=8

[5] DAVEK. Pretexing Like a Boss. In: *TrustedSec* [online]. 2014 [cit. 2016-04-09]. Dostupné z: https://www.trustedsec.com/march-2014/pretexting-like-boss/

[6] MIJARES, Alejandro. *Social engineering: Employees could be your weakest link* [online]. , 2 [cit. 2016-04-09]. Dostupné z: http://www.computerworld.com/article/2996606/cybercrime-hacking/social-engineering-employees-could-be-your-weakest-link.html

[7] CRYSSMAN. Ukázka typického phishing e-mailu s vysvětlením. *Wikipedia* [online]. [cit. 2016-05-19]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Phishing&oldid=13356873#/media/File:Jak_snadno_poznat_phishing.png

[8] MCDOWELL, Mindi. Avoiding Social Engineering and Phishing Attacks. In: *US-CERT* [online]. [cit. 2016-04-09]. Dostupné z: https://www.us-cert.gov/ncas/tips/ST04-014

[9] Social Engineering: Would You Take the Bait? In: *Dara Security* [online]. [cit. 2016-04-09]. Dostupné z: https://www.darasecurity.com/article.php?id=32

[10] Social Engineering: : What is baiting? In: *Blog Mailfence* [online]. [cit. 2016-04-09]. Dostupné z: https://blog.mailfence.com/2015/11/18/what-is-baiting-in-social-engineering/

[11] KEYWORTH, Marie. Vishing and smishing: The rise of social engineering fraud. *BBC News* [online]. , 6 [cit. 2016-04-09]. Dostupné z: http://www.bbc.com/news/business-35201188

[12] BRISSON, David. 5 Social Engineering Attacks to Watch Out For. In: *TripWire* [online]. [cit. 2016-04-09]. Dostupné z: http://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/

[13] CHARLEY, Craig. Management the Steve Jobs way - Learning from Steve Jobs' Management Style. In: *Silicon Beach Training* [online]. [cit. 2016-04-09]. Dostupné z: https://www.siliconbeachtraining.co.uk/blog/steve-jobs-management-style

[14] SANDINEJS. Newton Security TDAR mantrap with piggybacking detected. In: *Youtube* [online]. [cit. 2016-04-09]. Dostupné z: https://www.youtube.com/watch?v=CS3ufPRkXuk

[15] LORD, Nate. What is Social Engineering? Defining and Avoiding Common Social Engineering Threats. In: *Digital Guardian* [online]. [cit. 2016-04-09]. Dostupné z: https://digitalguardian.com/blog/what-social-engineering-defining-and-avoiding-common-social-engineering-threats

[16] EKMAN, Paul. *Odhalené emoce*. Jan Melvil Publishing, 2015. ISBN 9788087270813.

[17] MITCK, Kevin a William SIMON. *Umění klamu*. HELION, 2003. ISBN 83-7361-210-6.

[18] NAVARRO, Joe a Marvin KARLINS. *Jak prokouknout druhé lidi: Příručka bývalého experta FBI*. Grada, 2010. ISBN 978-80-247-3350-0.

[19] CIALDINI, B. Robert. *Zbraně vlivu*. Jan Melvil Publishing, 2012. ISBN 978-80-87270-32-5.

[20] MCLELLAN, Sarah. 10 Tips for Not Getting Arrested, Killed, or Sick Abroad. Infinite Legroom [online]. [cit. 2016-05-19]. Dostupné z: http://infinitelegroom.com/2013/10/16/10-tips-for-not-getting-arrested-killed-or-sick-abroad/

[21] BARROW, Johnny. 14 Body Language Rules You Need To Know Before The Interview. *Rate My Job* [online]. [cit. 2016-05-19]. Dostupné z: http://www.ratemyjob.com/career/36261/14-body-language-rules-you-need-to-know-before-the-interview#slide/4

[22] B, Jessica. Week Five - Face of depression. *Rate My Job* [online]. [cit. 2016-05-19]. Dostupné z: https://www.flickr.com/photos/jessia-hime/3038466793

[23] ARBAOUI, Larbi. *The concept of Hshuma (shame) in Moroccan society* [online]. [cit. 2016-05-19]. Dostupné z: http://www.moroccoworldnews.com/2013/09/104788/the-concept-of-hshuma-shame-in-moroccan-society/

[24] EKMAN, Paul. *Emoce pod maskou*. BIZBOOKS, 2015. ISBN 9788026504221

SEZNAM OBRÁZKŮ

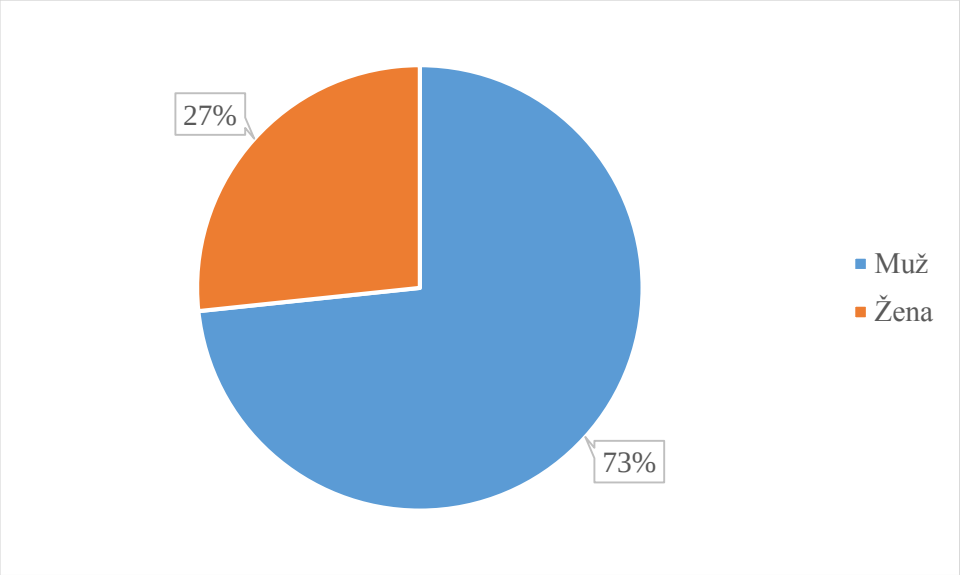
SEZNAM GRAFŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

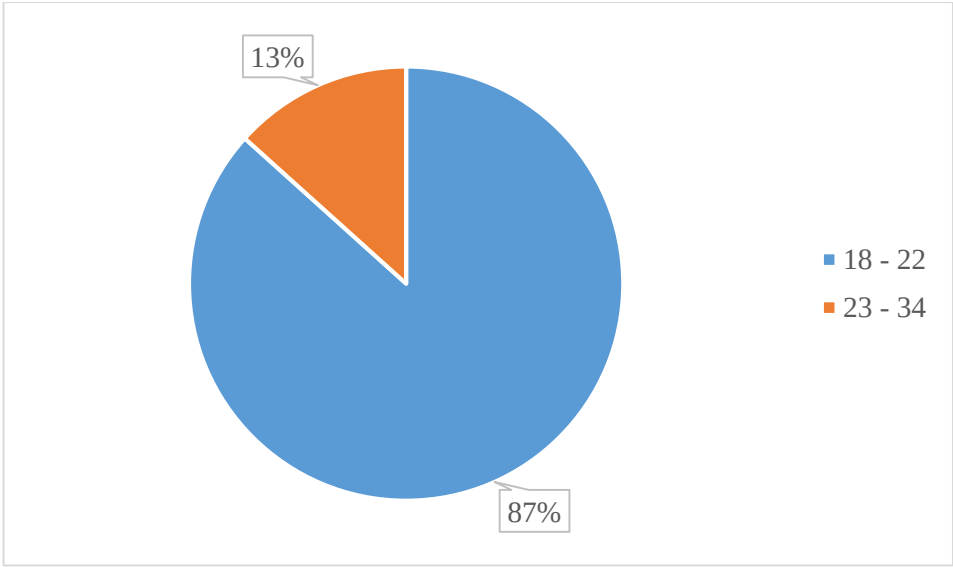
PŘÍLOHA P1: ZKUŠENOST S DOTAZNÍKY – PÍSEMNÁ FORMA

1) Jste muž nebo žena?



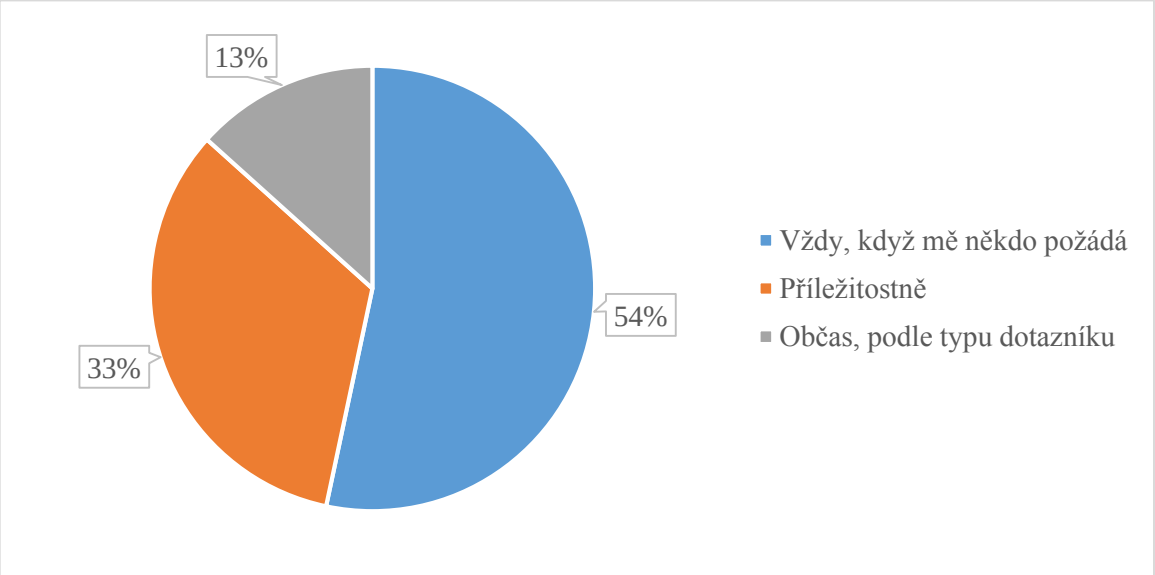
Odpovědi	Respondenti	Podíl
Muž	11	73%
Žena	4	27%

2) Věk?



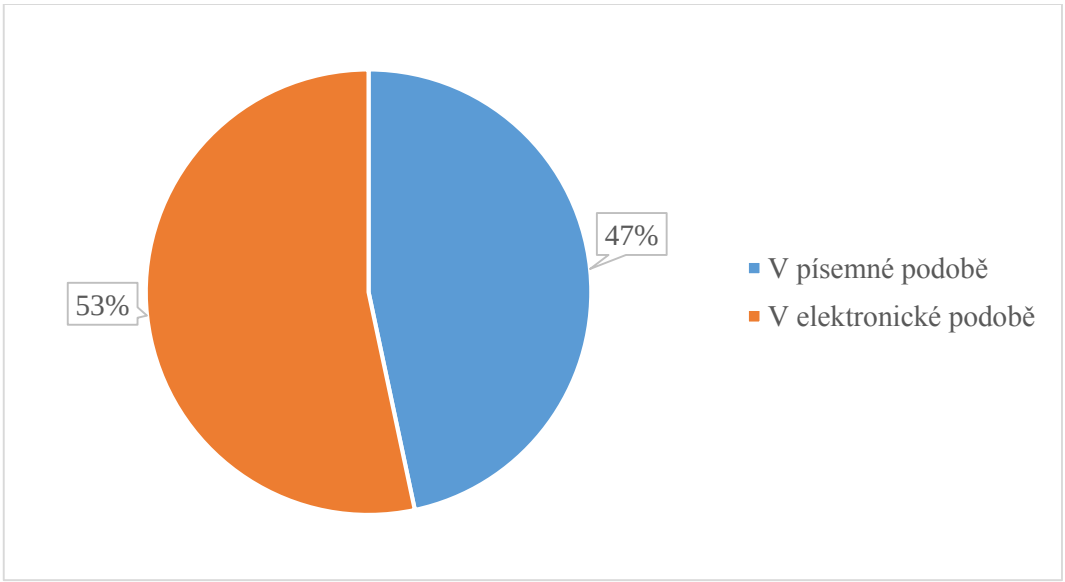
Odpovědi	Respondenti	Podíl
14 - 17	0	0%
18 - 22	13	87%
23 - 34	2	13%
35 - 45	0	0%
46 a víc	0	0%

3) Jak často vyplňujete dotazníky? Zkuste odhadnout, jak často.



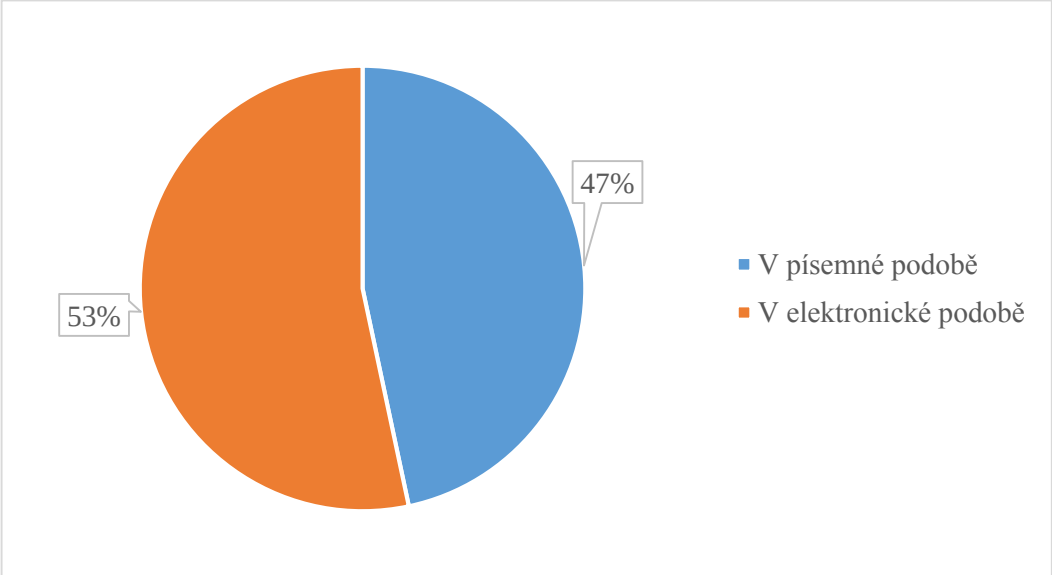
Odpovědi	Respondenti	Podíl
Vždy, když mě někdo požádá	8	54%
Příležitostně	5	33%
Občas, podle typu dotazníku	2	13%

4) V jaké podobě se s dotazníky nejčastěji setkáváte?



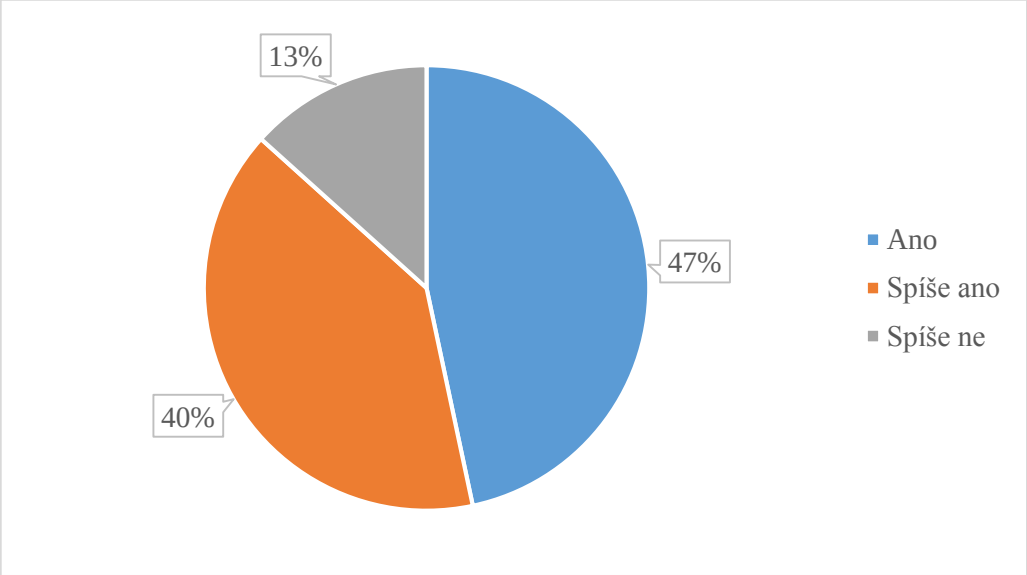
Odpovědi	Respondenti	Podíl
V písemné podobě	7	47 %
V elektronické podobě	8	53 %
Po telefonu		0%

5) Jaká podoba dotazníku je pro vás přijatelnější?



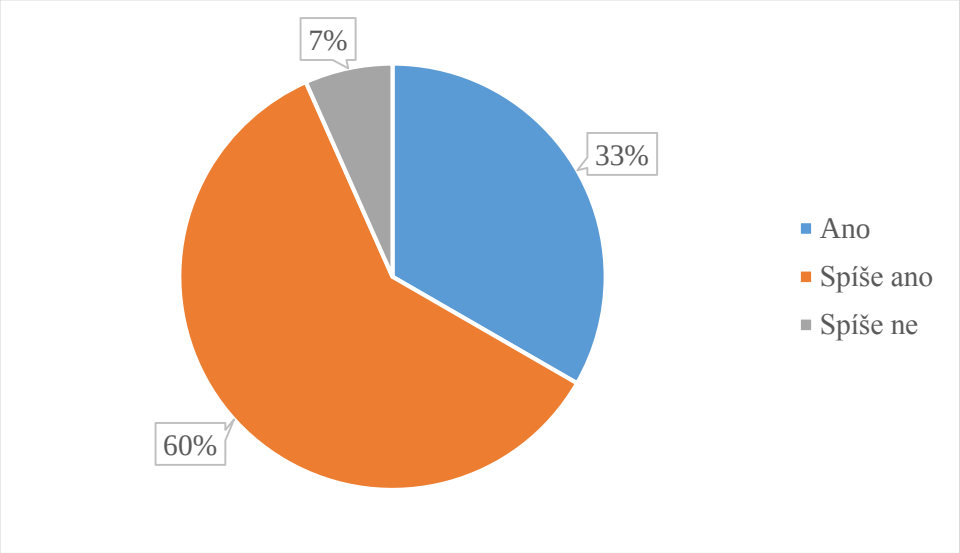
Odpovědi	Respondenti	Podíl
V písemné podobě	7	47%
V elektronické podobě	8	53%
Po telefonu	0	0%

6) Myslíte si, že dotazníky mají obecně nějaký přínos?



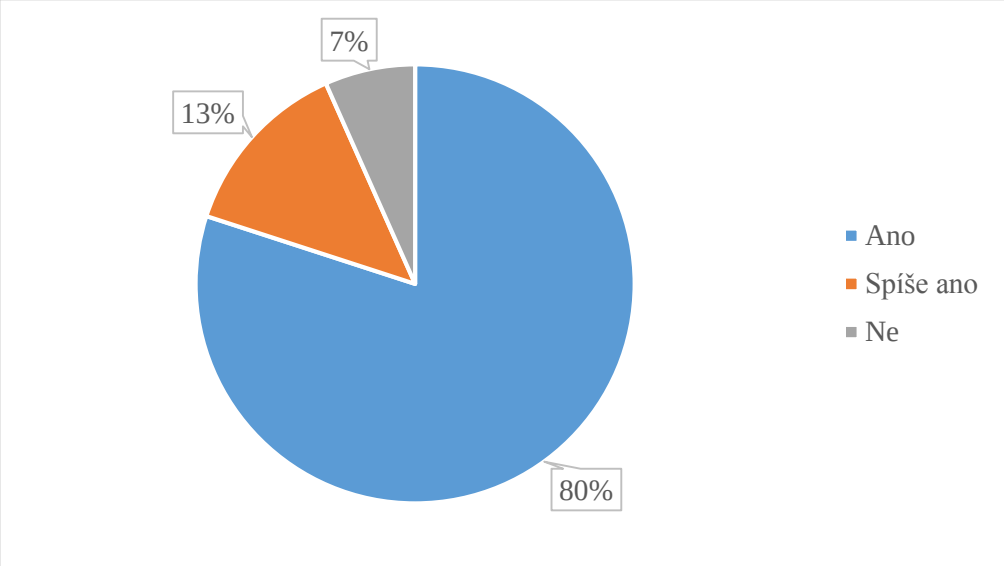
Odpovědi	Respondenti	Podíl
Ano	7	47%
Spíše ano	6	40%
Spíše ne	2	13%
Ne	0	0%

7) Myslíte si, že výstupní hodnoty z dotazníků jsou důvěryhodné a dá se s nimi dál pracovat?



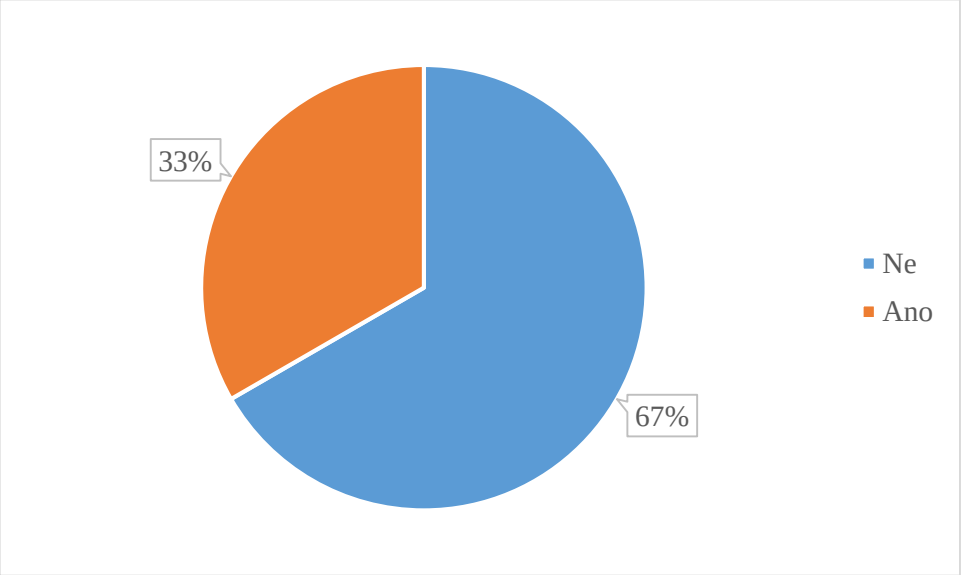
Odpovědi	Respondenti	Podíl
Ano	5	33%
Spíše ano	9	60%
Spíše ne	1	7%
Ne	0	0%

8) Vyplňujete dotazníky pravdivě?



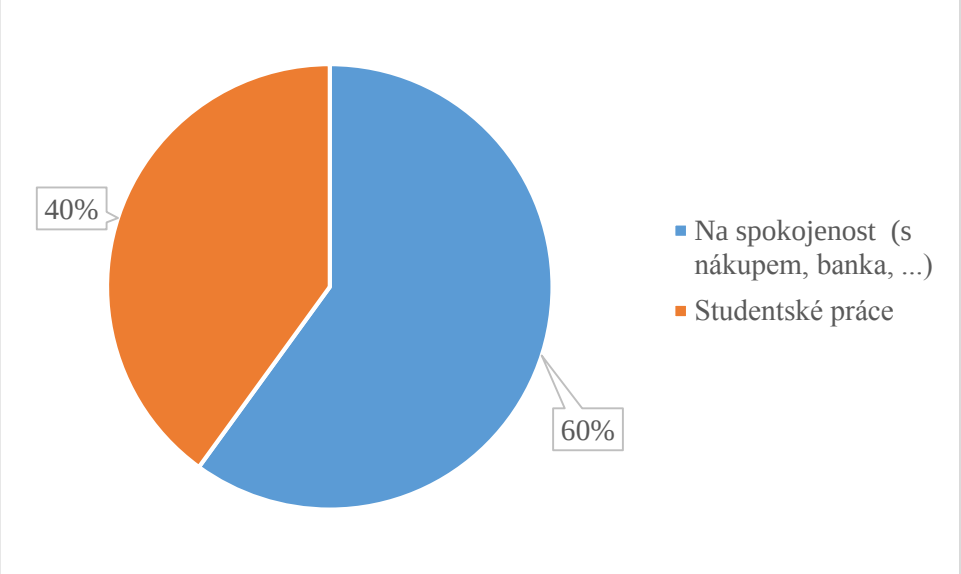
Odpovědi	Respondenti	Podíl
Ano	12	80%
Spíše ano	2	13%
Spíše ne	0	0%
Ne	1	7%

9) Sdělili byste soukromé informace (např. jméno, výdělek, adresu, ...) v rámci dotazníku? Pokud ano, které?



Odpovědi	Respondenti	Podíl
Ne	10	67%
Ano	5	33%

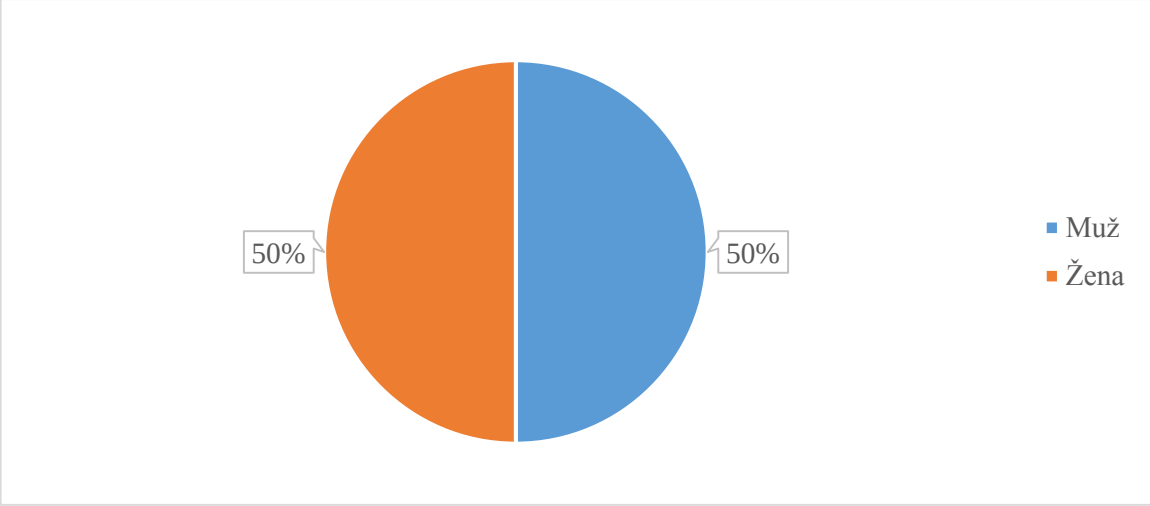
10) Jaké zaměření mají obvykle dotazníky, které vyplňujete?



Odpovědi	Respondenti	Podíl
Na frekvenci nákupu	0	0%
Na spokojenost (s nákupem, banka, ...)	9	40%
Studentské práce	6	60%

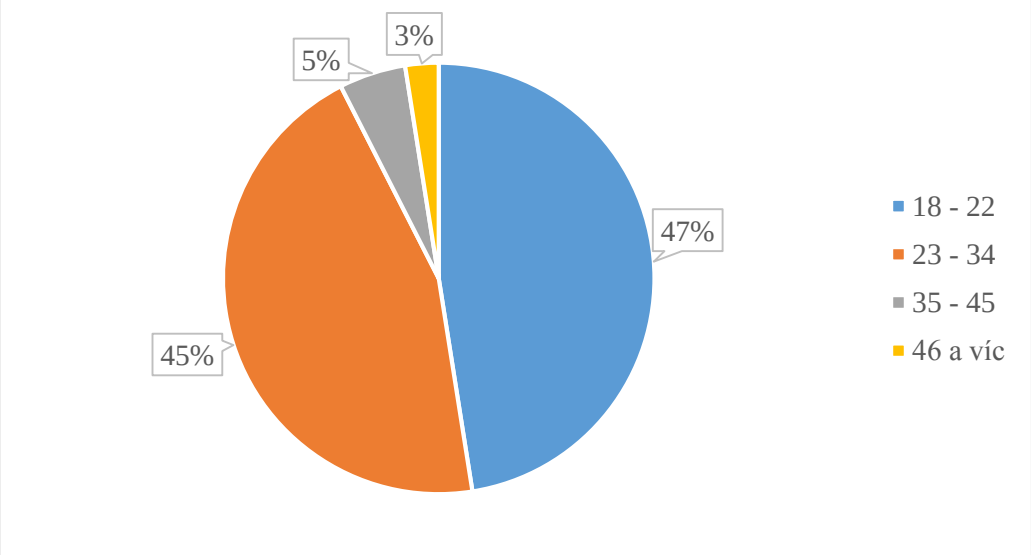
PŘÍLOHA P2: ZKUŠENOST S DOTAZNÍKY – ELEKTORNICKÁ FORMA

1) Jste muž nebo žena?



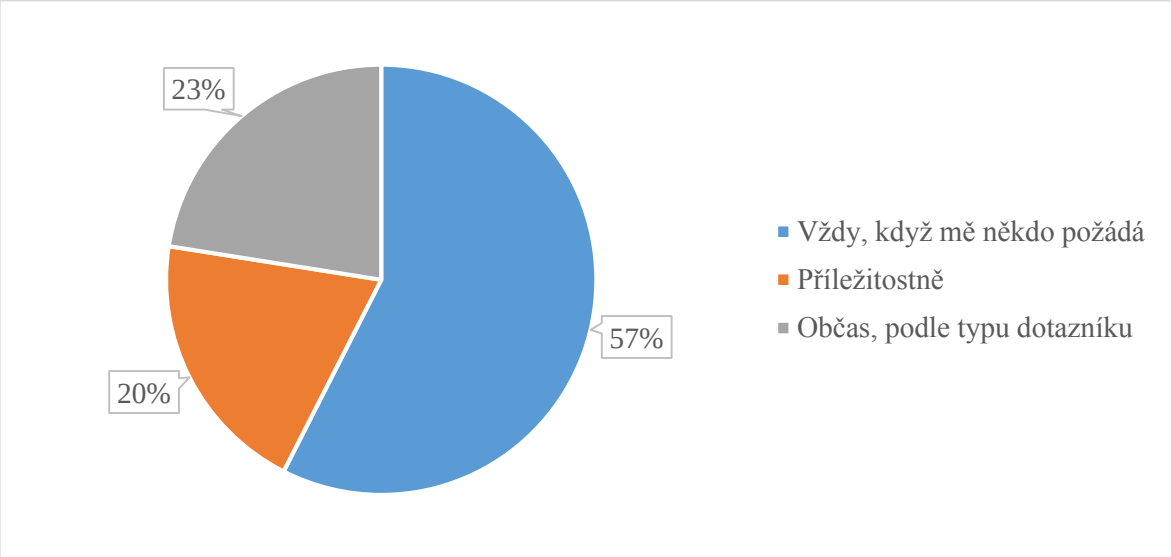
Odpovědi	Respondenti	Podíl
Muž	20	50%
Žena	20	50%

2) Věk?



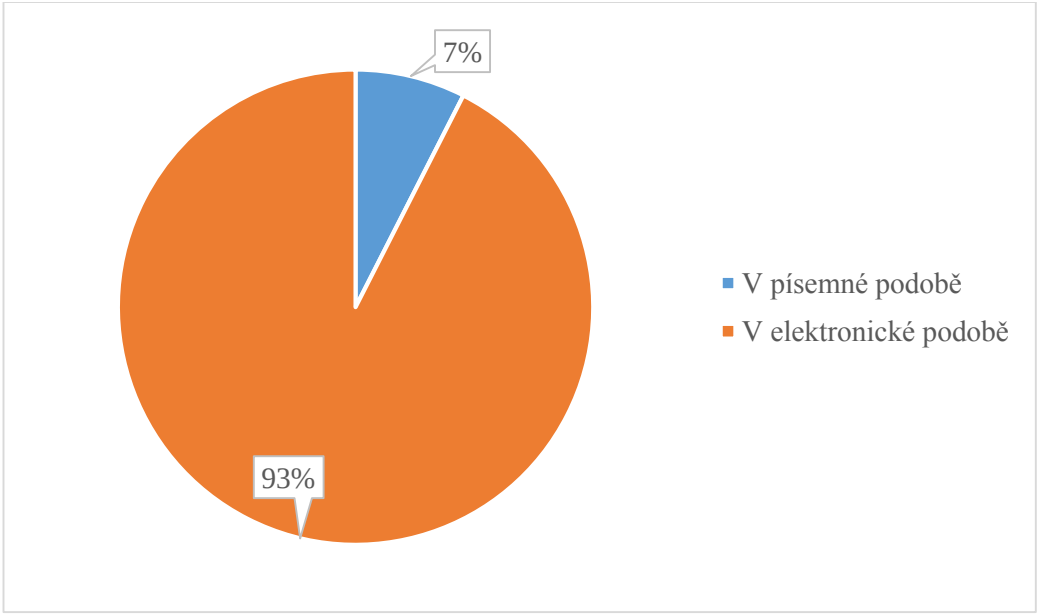
Odpovědi	Respondenti	Podíl
14 - 17	0	0%
18 - 22	19	47%
23 - 34	18	45%
35 - 45	2	5%
46 a víc	1	3%

3) Jak často vyplňujete dotazníky? Zkuste odhadnout, jak často.



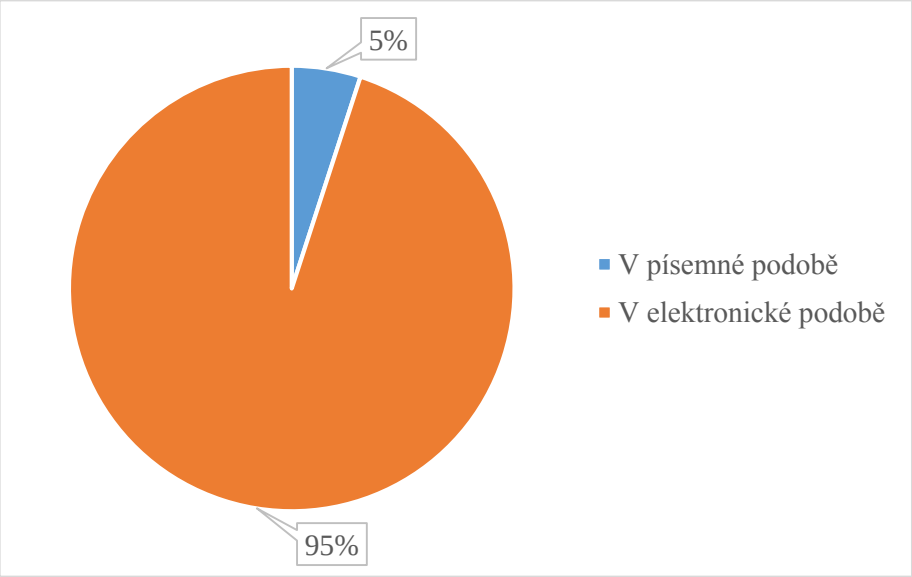
Odpovědi	Respondenti	Podíl
Vždy, když mě někdo požádá	23	57%
Příležitostně	8	20%
Občas, podle typu dotazníku	9	23%

4) V jaké podobě se s dotazníky nejčastěji setkáváte?



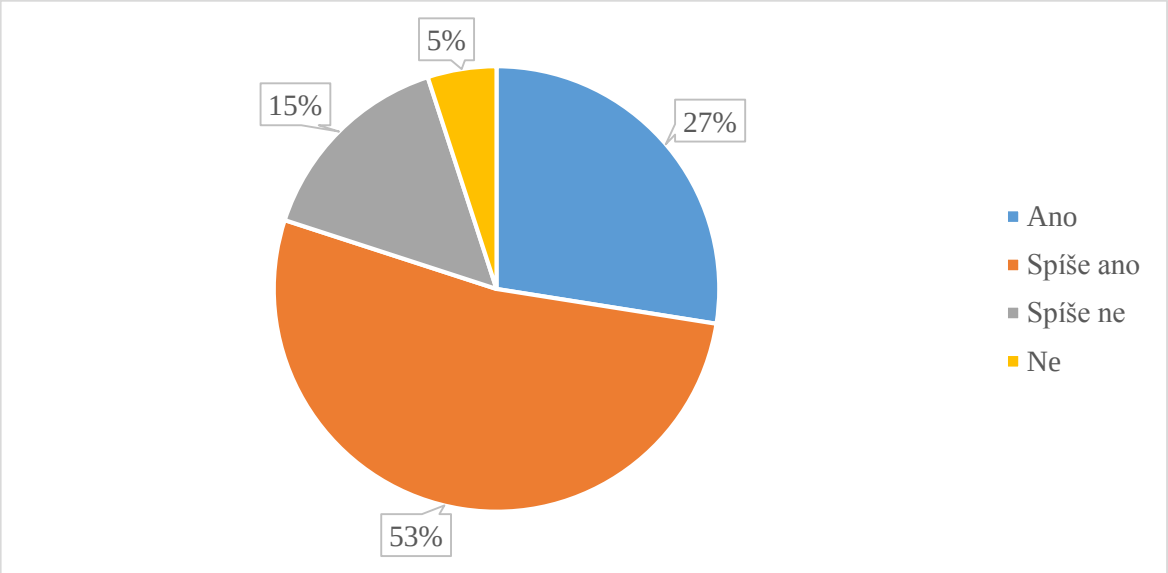
Odpovědi	Respondenti	Podíl
V písemné podobě	3	7 %
V elektronické podobě	37	93 %
Po telefonu	0	0%

5) Jaká podoba dotazníku je pro vás přijatelnější?



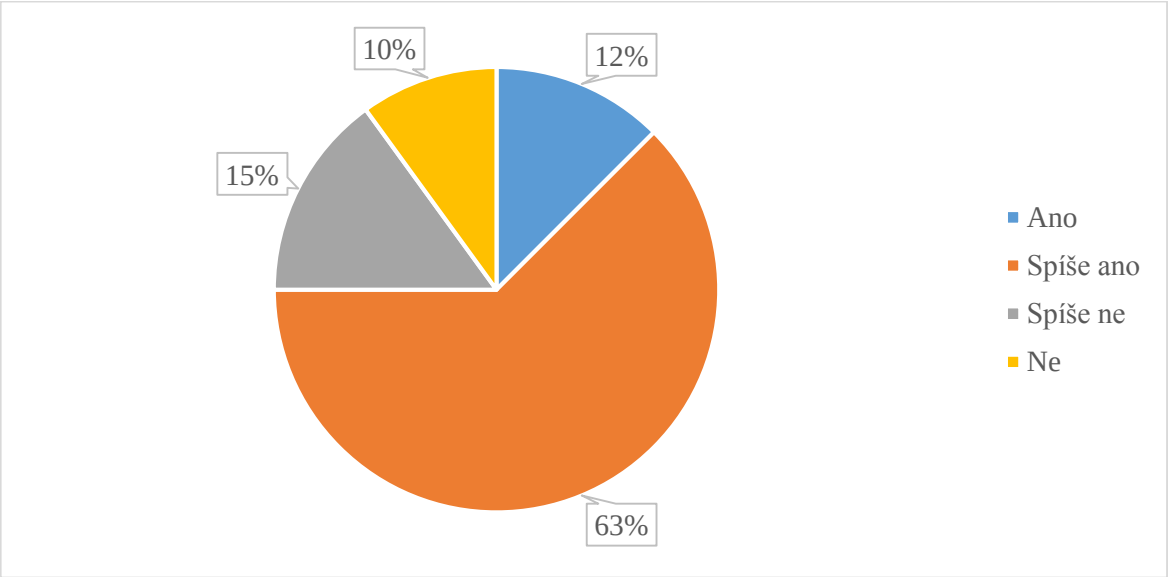
Odpovědi	Respondenti	Podíl
V písemné podobě	2	5 %
V elektronické podobě	38	95 %
Po telefonu	0	0%

6) Myslíte si, že dotazníky mají obecně nějaký přínos?



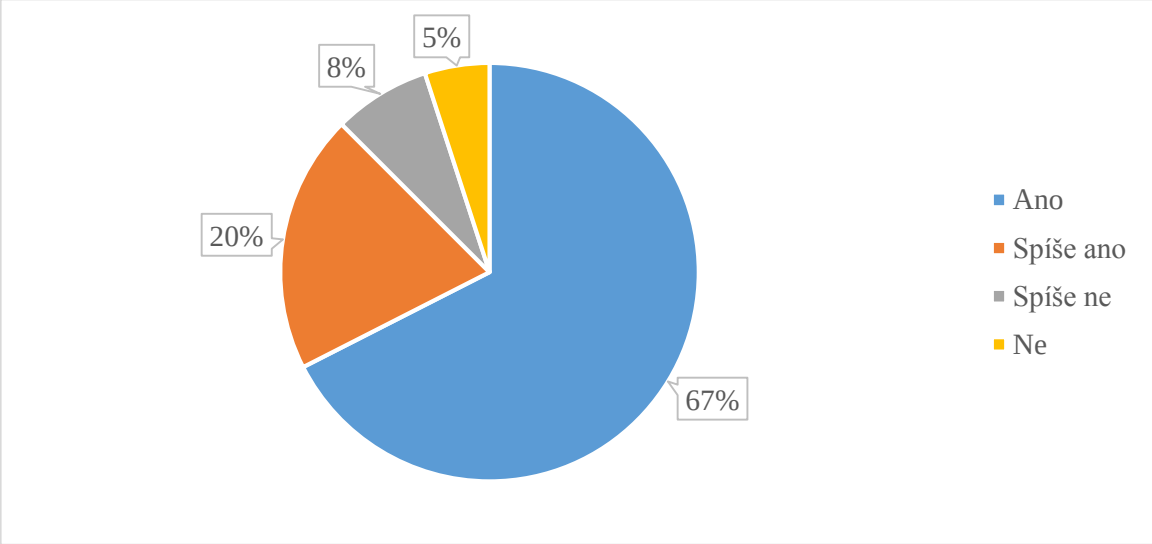
Odpovědi	Respondenti	Podíl
Ano	11	27,5 %
Spíše ano	21	52,5 %
Spíše ne	6	15 %
Ne	2	5 %

7) Myslíte si, že výstupní hodnoty z dotazníků jsou důvěryhodné a dá se s nimi dál pracovat?



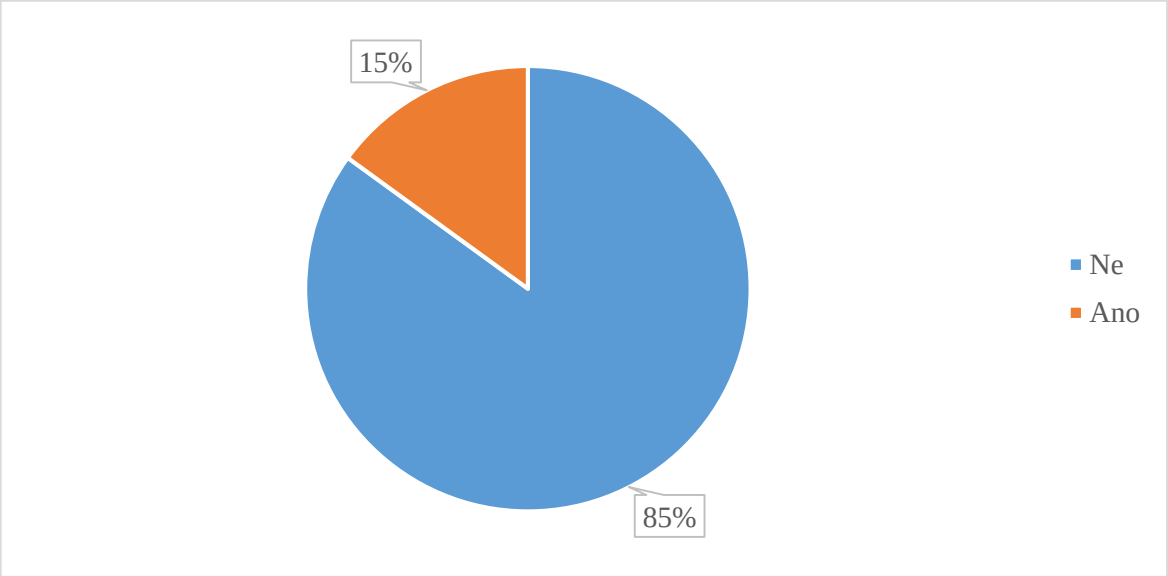
Odpovědi	Respondenti	Podíl
Ano	5	12,5 %
Spíše ano	25	62,5 %
Spíše ne	6	15 %
Ne	4	10 %

8) Vyplňujete dotazníky pravdivě?



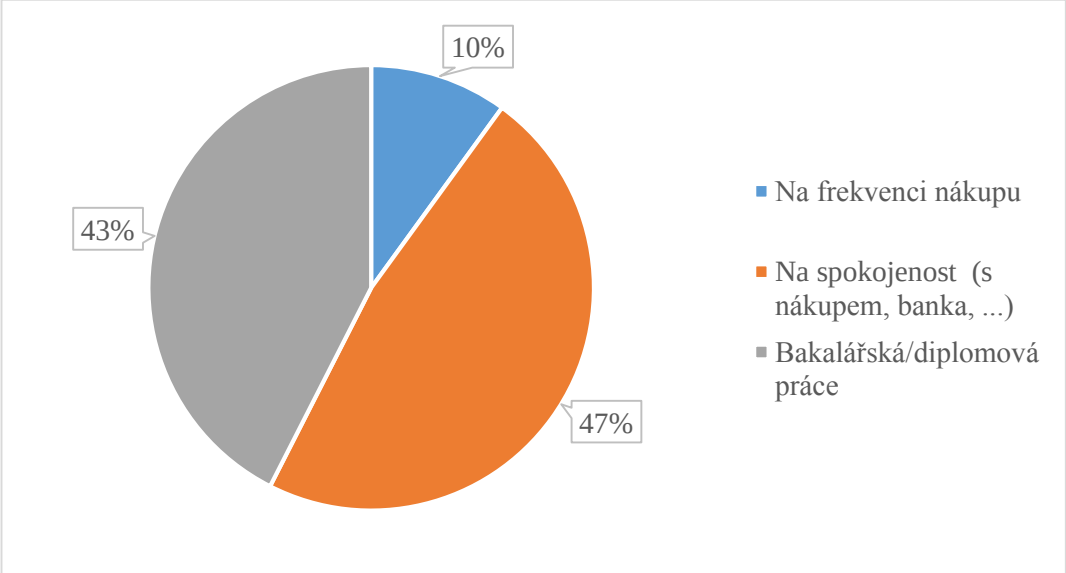
Odpovědi	Respondenti	Podíl
Ano	27	67 %
Spíše ano	8	20 %
Spíše ne	3	8 %
Ne	2	5%

9) Sdělili byste soukromé informace (např. jméno, výdělek, adresu, ...) v rámci dotazníku? Pokud ano, které?



Odpovědi	Respondenti	Podíl
Ne	34	85 %
Ano	6	15 %

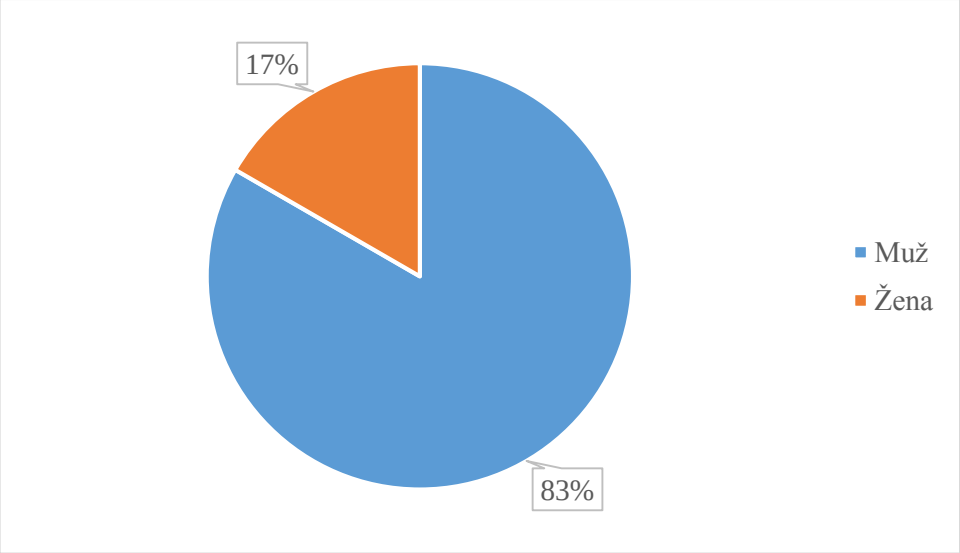
10) Jaké zaměření mají obvykle dotazníky, které vyplňujete?



Odpovědi	Respondenti	Podíl
Na frekvenci nákupu	4	10 %
Na spokojenost (s nákupem, banka, ...)	19	47 %
Studentské práce	17	43 %

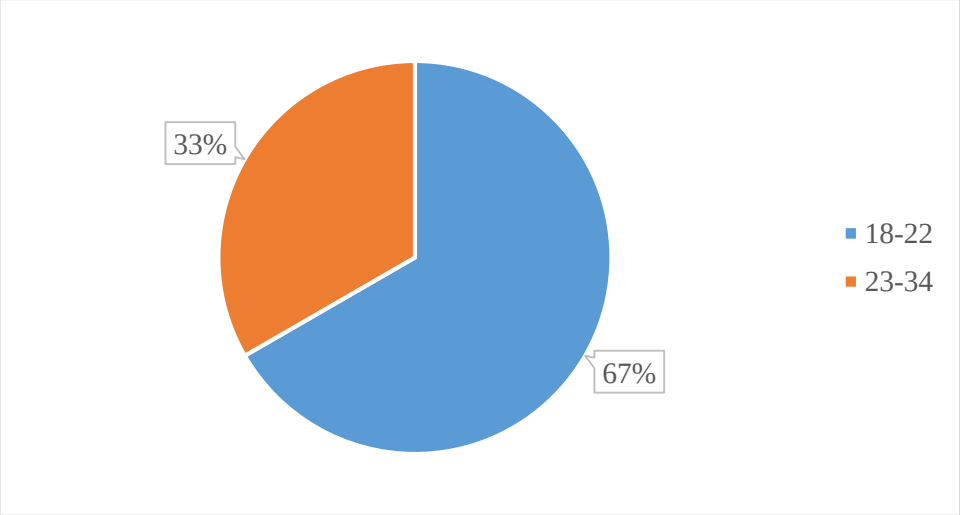
PŘÍLOHA P3: AUTA Z HLEDISKA ROZŠÍŘENOSTI – PÍSEMNÁ FORMA

1) Jste muž nebo žena?



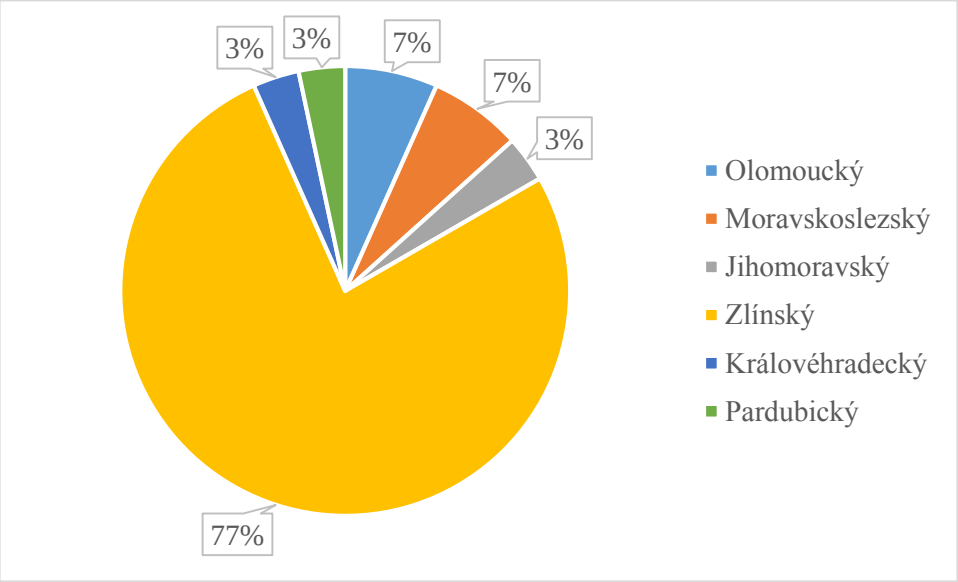
Odpovědi	Respondenti	Podíl
Muž	25	83%
Žena	5	17%

2) Věk?



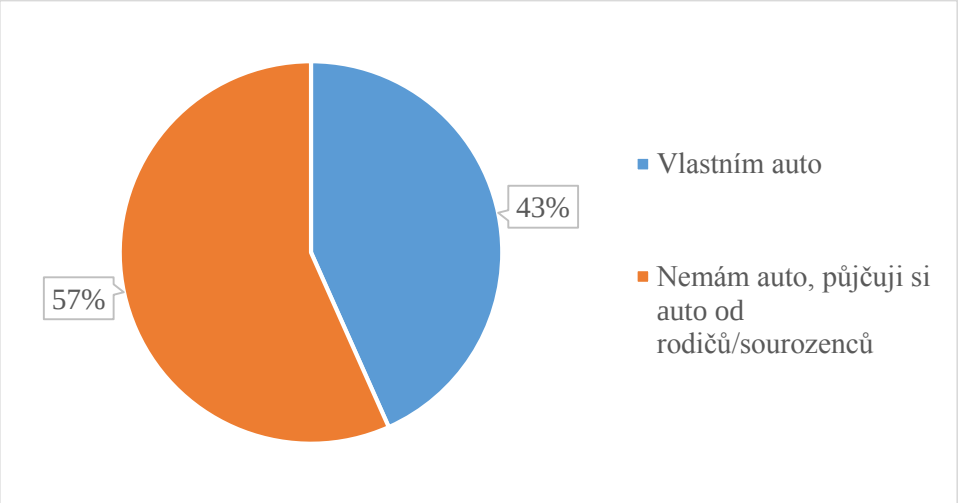
Odpovědi	Respondenti	Podíl
18-22	20	67%
23-34	10	33%
35-45	0	0%
46-55	0	0 %
56 a víc	0	0 %

3) Kraj?



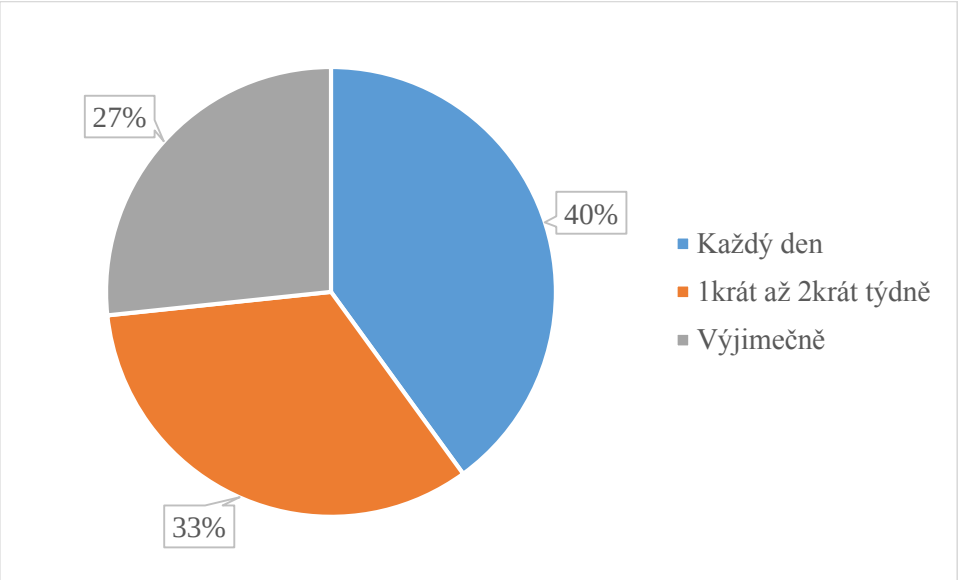
Odpovědi	Respondenti	Podíl
Hlavní město Praha	0	0 %
Olomoucký	2	7%
Moravskoslezský	2	7%
Jihomoravský	1	3%
Zlínský	23	77%
Kraj Vysočina	0	0 %
Středočeský	0	0 %
Jihočeský	0	0 %
Plzeňský	0	0 %
Karlovarský	0	0 %
Ústecký	0	0 %
Liberecký	0	0 %
Královéhradecký	1	3%
Pardubický	1	3%

4) Vlastníte auto nebo si půjčujete auto někoho jiného?



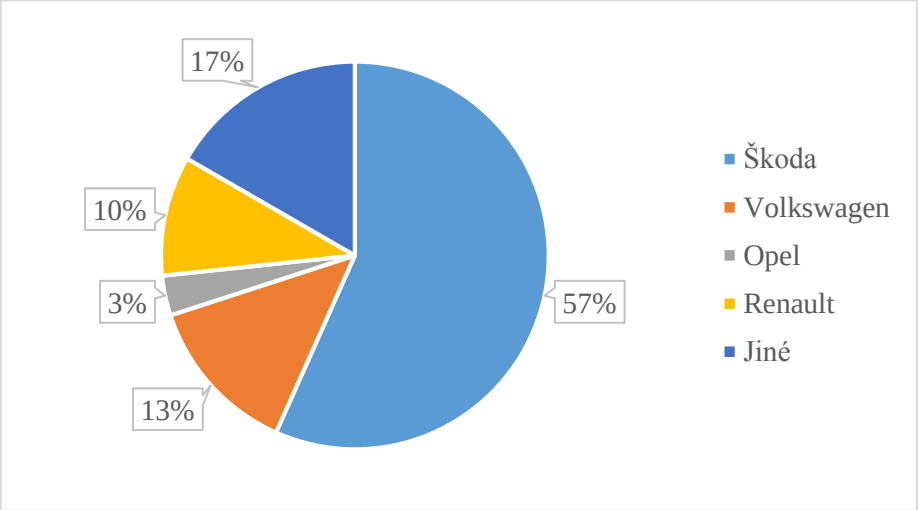
Odpovědi	Respondenti	Podíl
Vlastním auto	13	43%
Nemám auto, půjčuji si auto od kamaráda	0	0 %
Nemám auto, půjčuji si auto od rodičů/sourozenců	17	57%
Nemám auto, neřídím	0	0%
Sdílím auto s	0	0 %

5) Jak často řídíte?



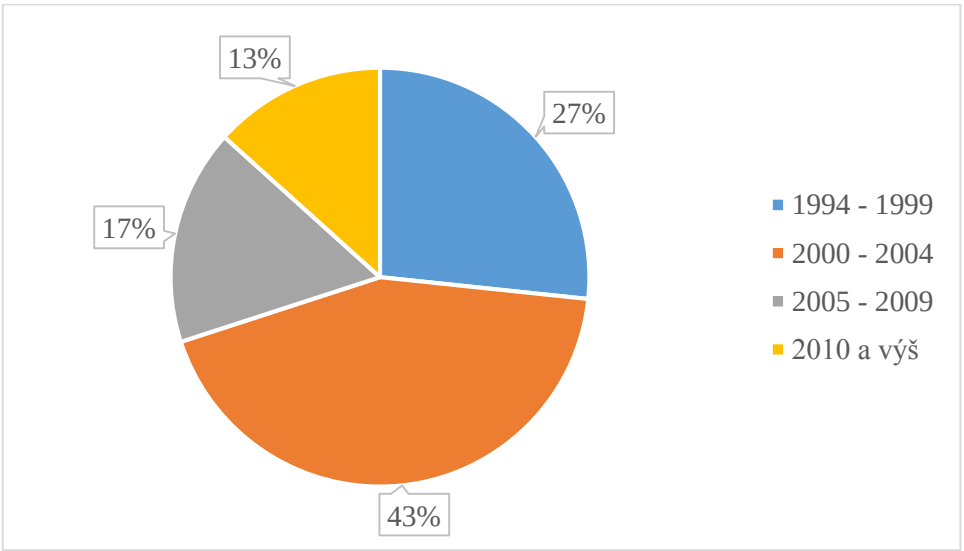
Odpovědi	Respondenti	Podíl
Každý den	12	47,4 %
Vždy, když je škola	0	21,1 %
Vždy, když jdu do práce	0	5,3 %
1krát až 2krát týdně	10	15,8 %
Výjimečně	8	10,5 %

6) Jaký typ auta řídíte?



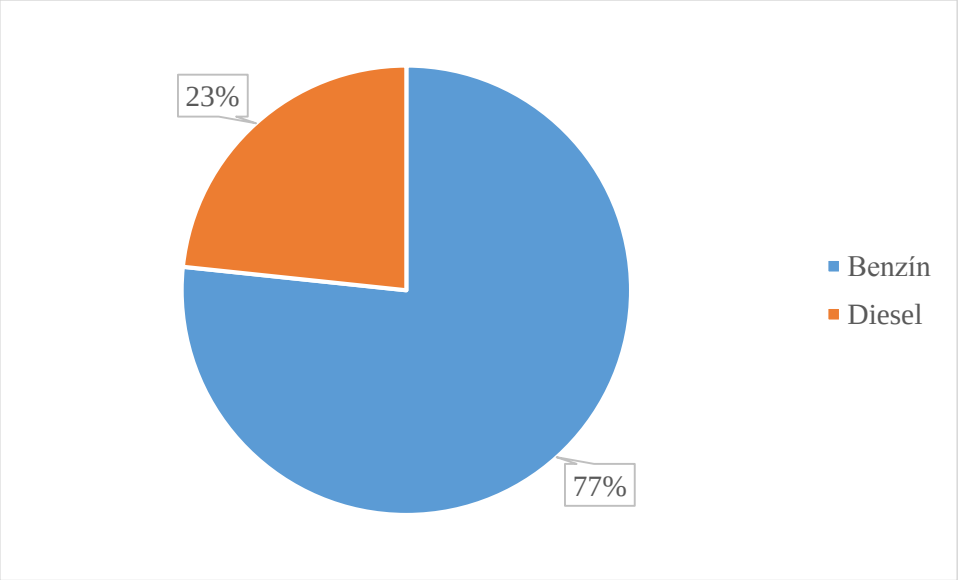
Odpovědi	Respondenti	Podíl
Škoda	17	57%
Volkswagen	4	13%
Ford	0	0%
Audi	0	0 %
Opel	1	3%
BMW	0	0%
Renault	3	10%
Fiat	0	0 %
Toyota	0	0%
Jiné	5	17%

7) Rok výroby auta?



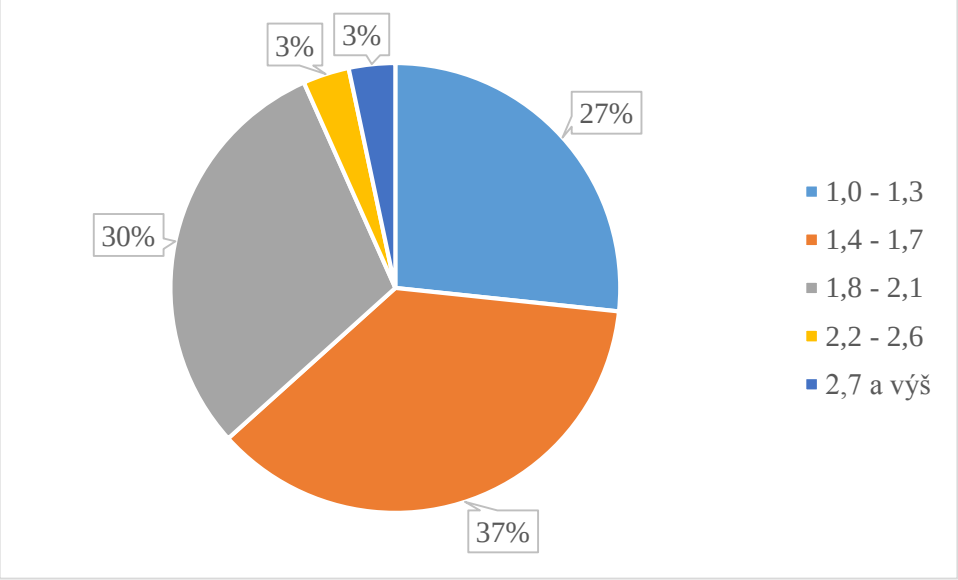
Odpovědi	Respondenti	Podíl
1994 - 1999	8	27%
2000 - 2004	13	43%
2005 - 2009	5	17%
2010 a výš	4	13%

8) Typ motoru?



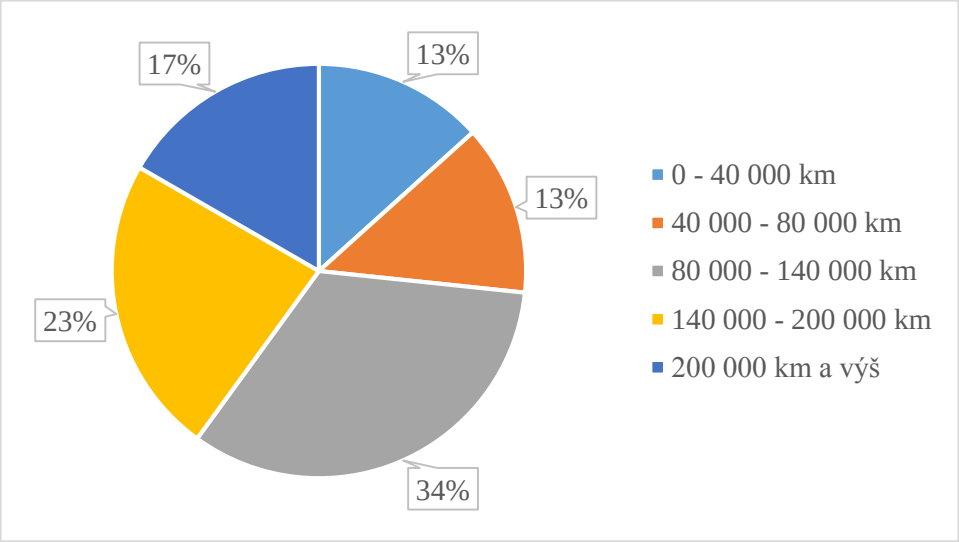
Odpovědi	Respondenti	Podíl
Benzín	23	77%
Diesel	7	23%
Kombinace s LPG	0	0 %

9) Obsah motoru? (Hodnoty jsou v litrech)



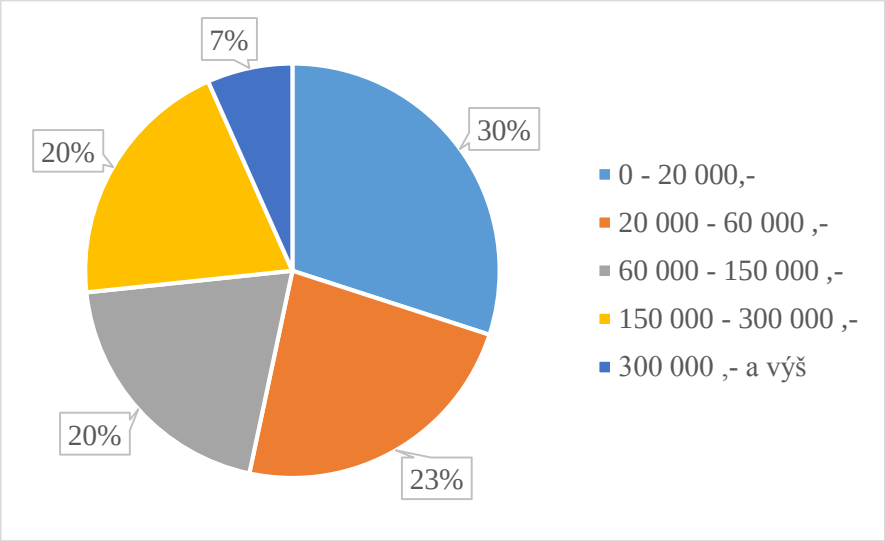
Odpovědi	Respondenti	Podíl
1,0 - 1,3	8	27%
1,4 - 1,7	11	37%
1,8 - 2,1	9	30%
2,2 - 2,6	1	3%
2,7 a výš	1	3%

10) Najeté kilometry?



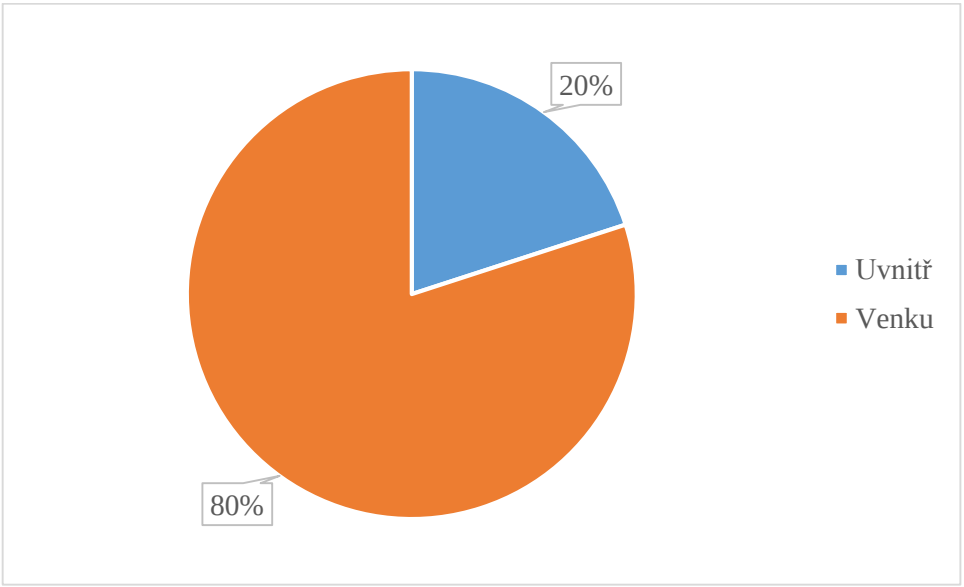
Odpovědi	Respondenti	Podíl
0 - 40 000 km	4	13%
40 000 - 80 000 km	4	13%
80 000 - 140 000 km	10	34%
140 000 - 200 000 km	7	23%
200 000 km a výš	5	17%

11) Odhadovaná cena auta?



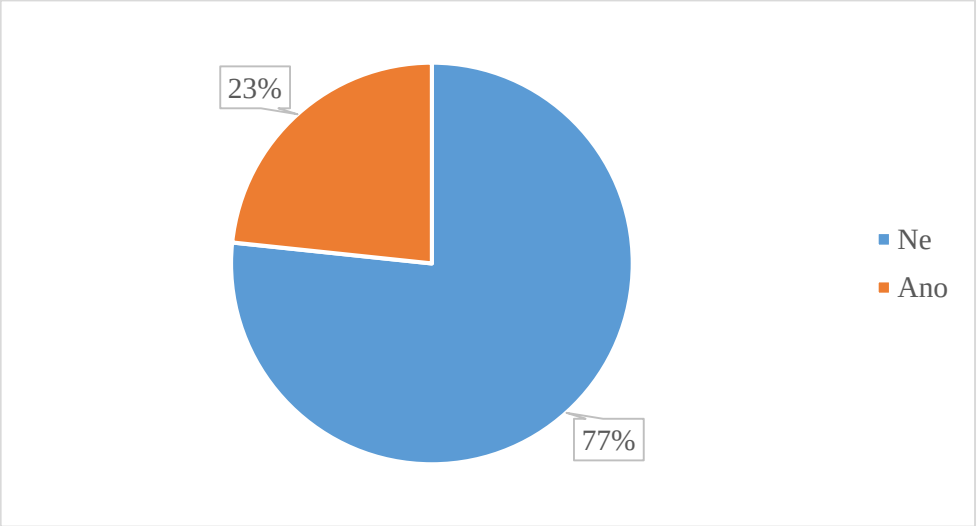
Odpovědi	Respondenti	Podíl
0 - 20 000,-	9	30%
20 000 - 60 000,-	7	23%
60 000 - 150 000,-	6	20%
150 000 - 300 000,-	6	20%
300 000,- - a výš	2	7%

12) Parkujete spíše uvnitř/venku?



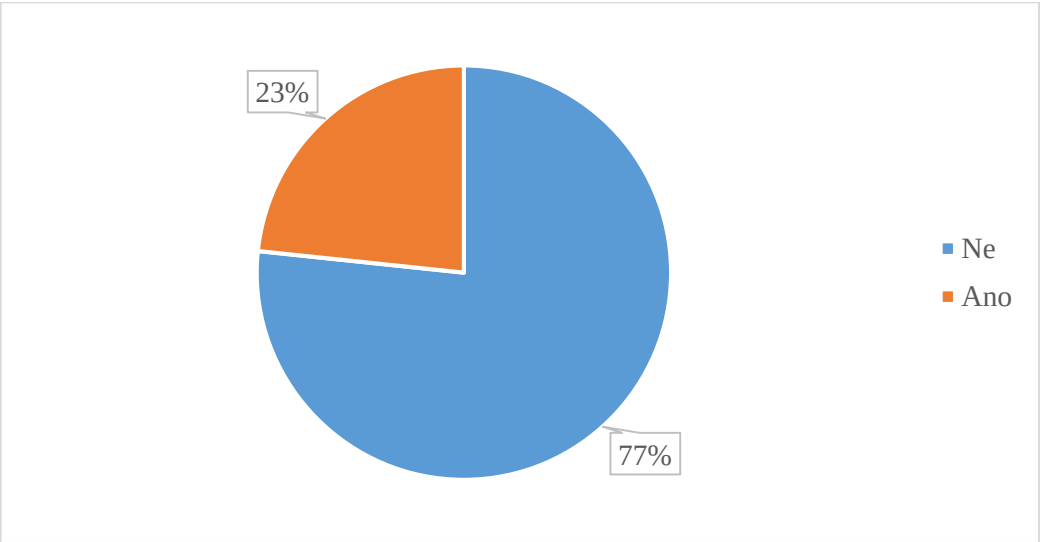
Odpovědi	Respondenti	Podíl
Uvnitř	6	20%
Venku	24	80%

13) V jaké lokalitě parkujete?



Odpovědi	Respondenti	Podíl
Sídliště	5	17%
Hlídané parkoviště	0	0 %
U obchodního centra	0	0 %
Garáž	7	23%
Před domem	18	60%
Jinde	0	0 %

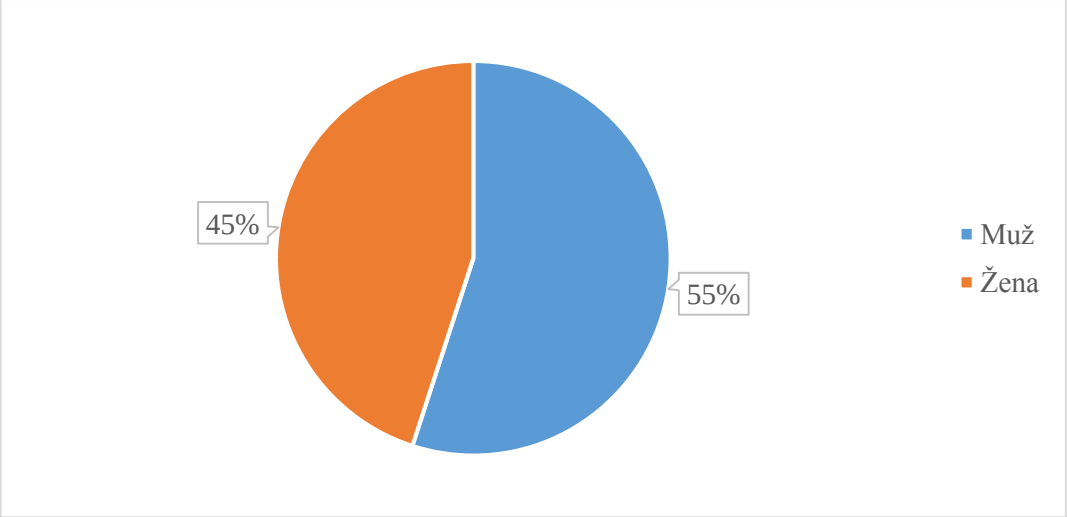
14) Má dané auto nějaké zabezpečení, které není v základní výbavě auta? Pokud ano, jaké? (Zámek pedálů, volantu, GPS ...)



Odpovědi	Respondenti	Podíl
Ne	23	77%
Ano	7	23%

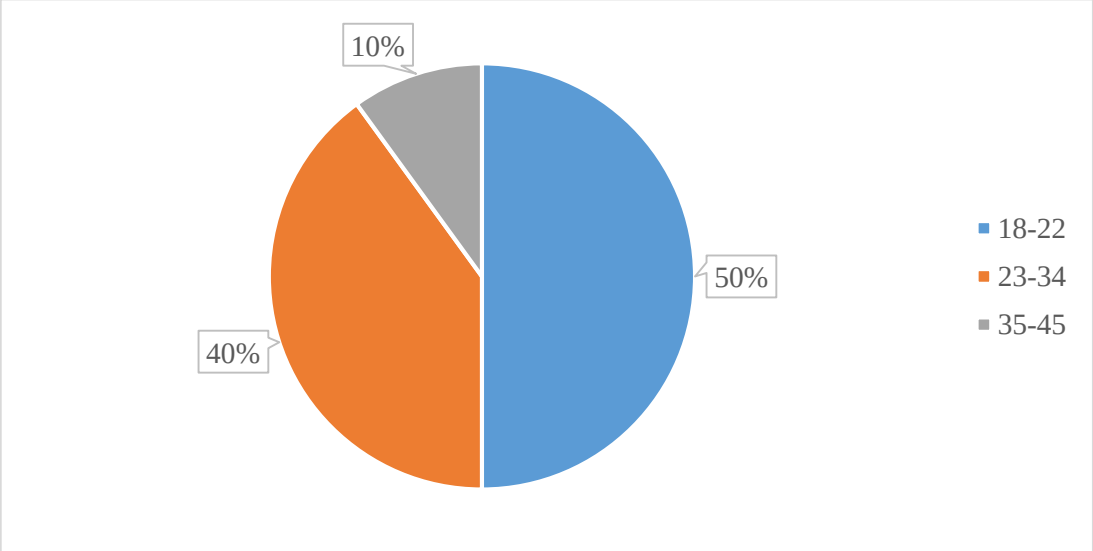
PŘÍLOHA P4: AUTA Z HLEDISKA ROZŠÍŘENOSTI – ELEKTRONICKÁ FORMA

1) Jste muž nebo žena?



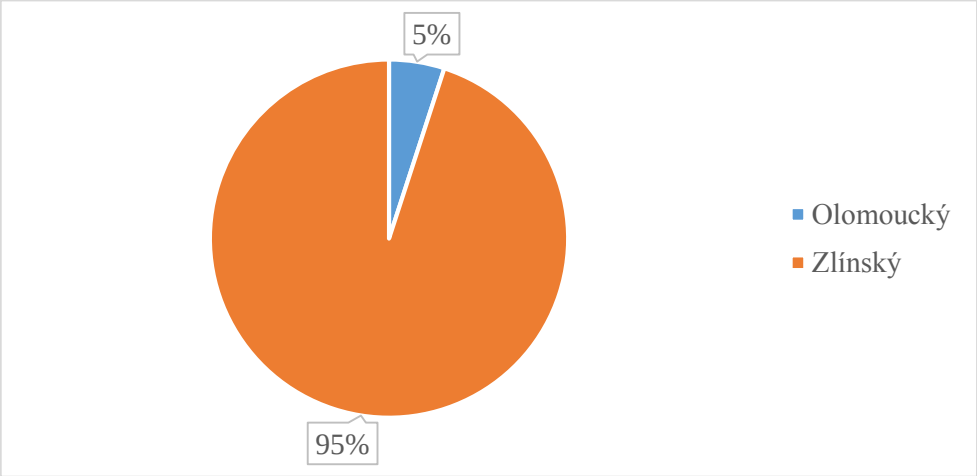
Odpovědi	Respondenti	Podíl
Muž	11	55%
Žena	9	45%

2) Věk?



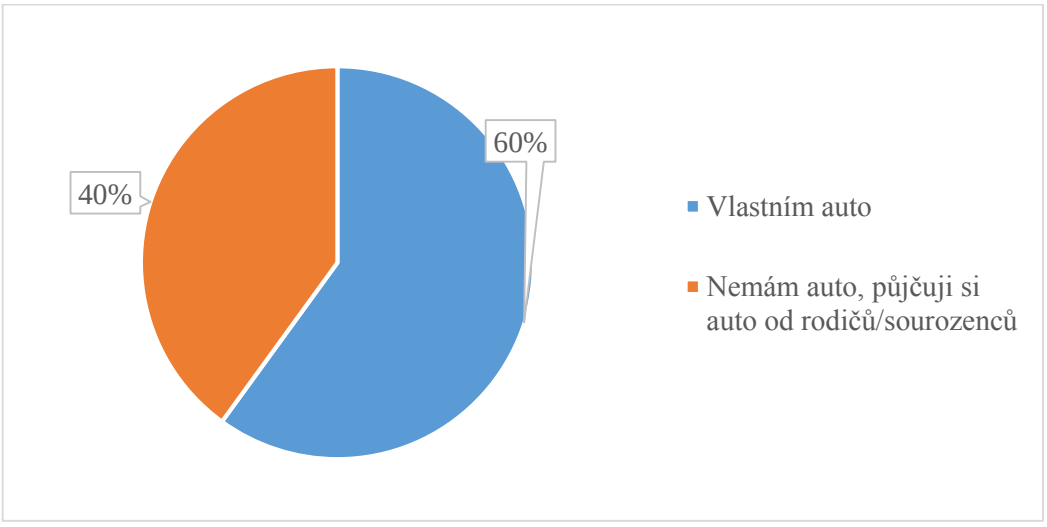
Odpovědi	Respondenti	Podíl
18-22	10	50%
23-34	8	40%
35-45	2	10%
46-55	0	0 %
56 a víc	0	0 %

3) Kraj?



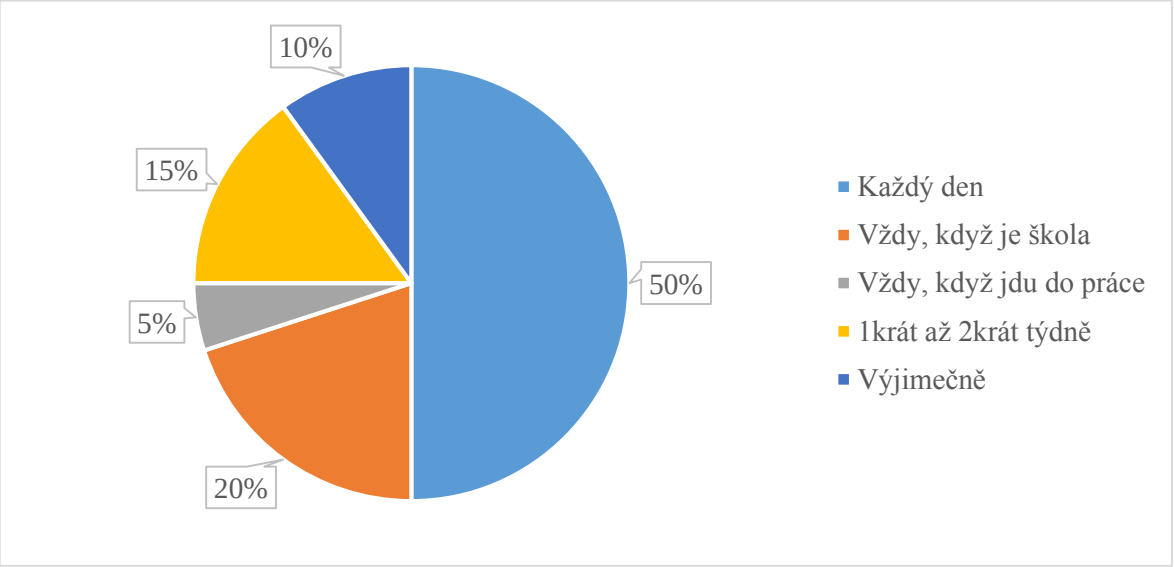
Odpovědi	Respondenti	Podíl
Hlavní město Praha	0	0 %
Olomoucký	1	5%
Moravskoslezský	0	0 %
Jihomoravský	0	0 %
Zlínský	19	95%
Kraj Vysočina	0	0 %
Středočeský	0	0 %
Jihočeský	0	0 %
Plzeňský	0	0 %
Karlovarský	0	0 %
Ústecký	0	0 %
Liberecký	0	0 %
Královéhradecký	0	0 %
Pardubický	0	0 %

4) Vlastníte auto nebo si půjčujete auto někoho jiného?



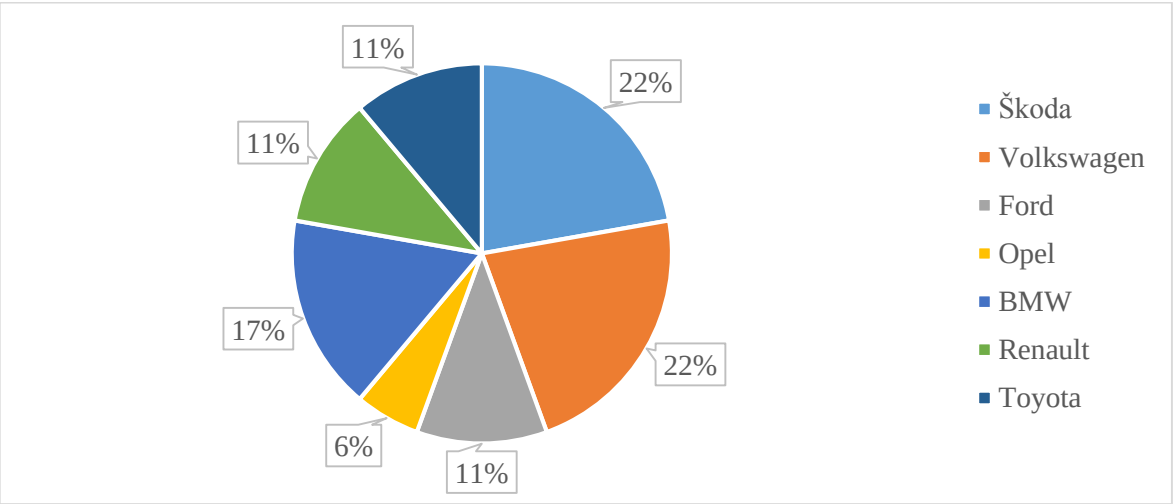
Odpovědi	Respondenti	Podíl
Vlastním auto	12	60%
Nemám auto, půjčuji si auto od kamaráda	0	0 %
Nemám auto, půjčuji si auto od rodičů/sourozenců	8	40%
Nemám auto, neřídím	0	0%
Sdílím auto s	0	0 %

5) Jak často řídíte?



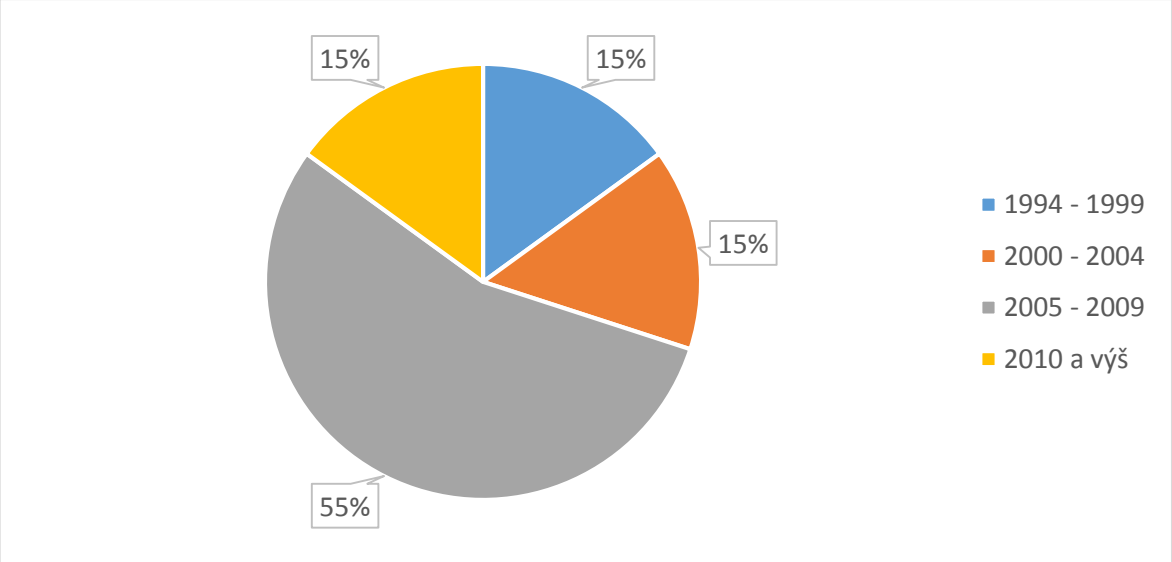
Odpovědi	Respondenti	Podíl
Každý den	10	47,4 %
Vždy, když je škola	4	21,1 %
Vždy, když jdu do práce	1	5,3 %
1krát až 2krát týdně	3	15,8 %
Výjimečně	2	10,5 %

6) Jaký typ auta řídíte?



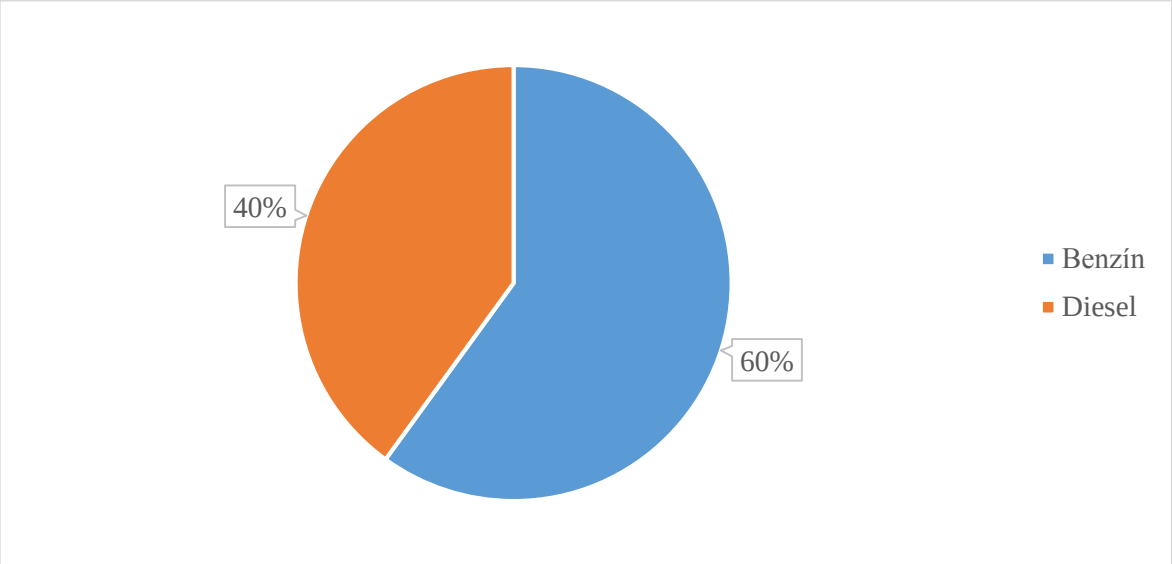
Odpovědi	Respondenti	Podíl
Škoda	4	22%
Volkswagen	4	22%
Ford	2	11%
Audi	0	0 %
Opel	1	6%
BMW	3	17%
Renault	2	11%
Fiat	0	0 %
Toyota	2	11%
Jiné	2	11%

7) Rok výroby auta?



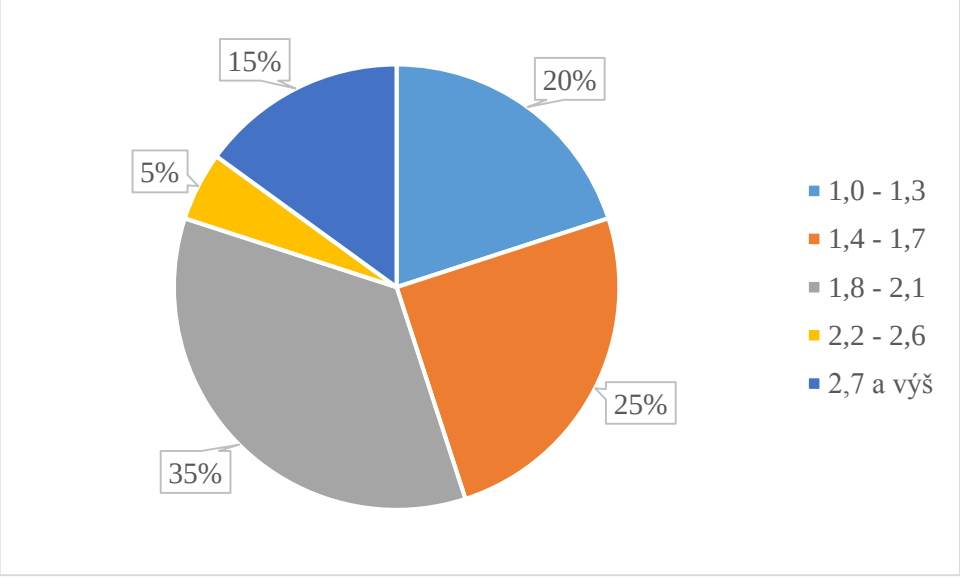
Odpovědi	Respondenti	Podíl
1994 - 1999	3	15%
2000 - 2004	3	15%
2005 - 2009	11	55 %
2010 a výš	3	15%

8) Typ motoru?



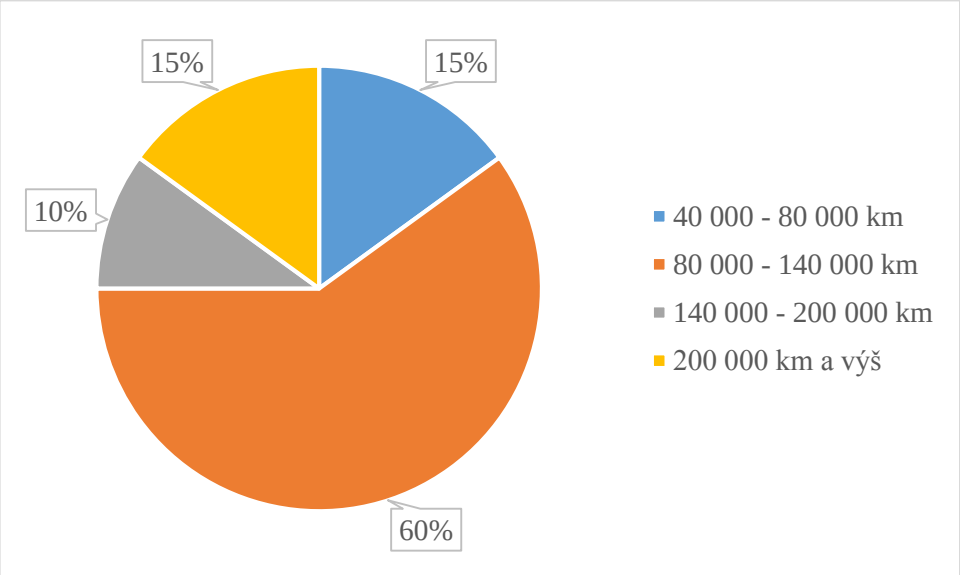
Odpovědi	Respondenti	Podíl
Benzín	12	60%
Diesel	8	40%
Kombinace s LPG	0	0 %

9) Obsah motoru? (Hodnoty jsou v litrech)



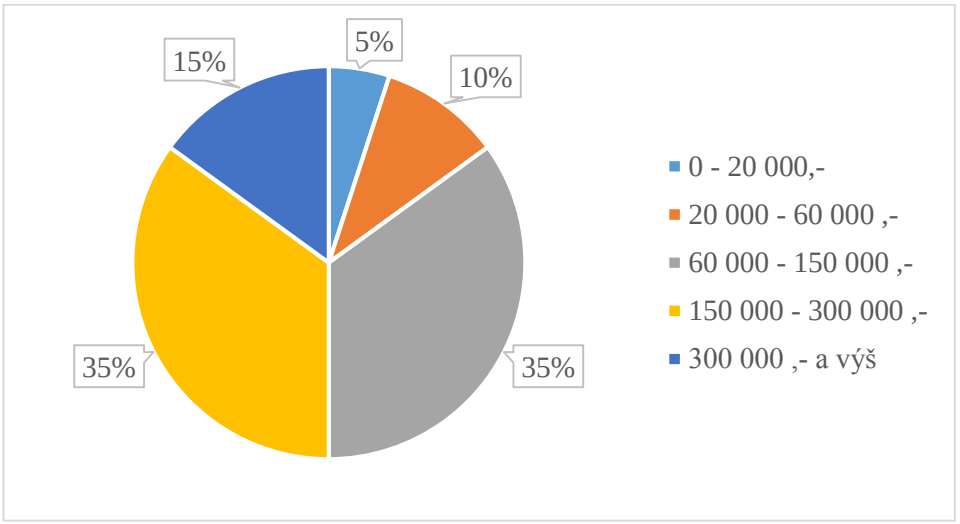
Odpovědi	Respondenti	Podíl
1,0 - 1,3	4	20%
1,4 - 1,7	5	25%
1,8 - 2,1	7	35%
2,2 - 2,6	1	5%
2,7 a výš	3	15%

10) Najeté kilometry?



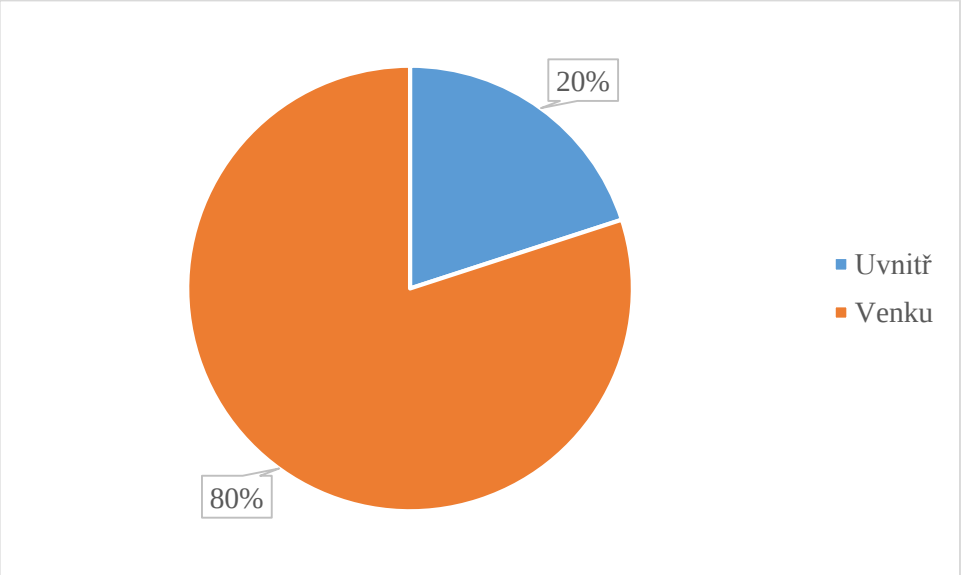
Odpovědi	Respondenti	Podíl
0 - 40 000 km	0	0 %
40 000 - 80 000 km	3	15%
80 000 - 140 000 km	12	60%
140 000 - 200 000 km	2	10%
200 000 km a výš	3	15%

11) Odhadovaná cena auta?



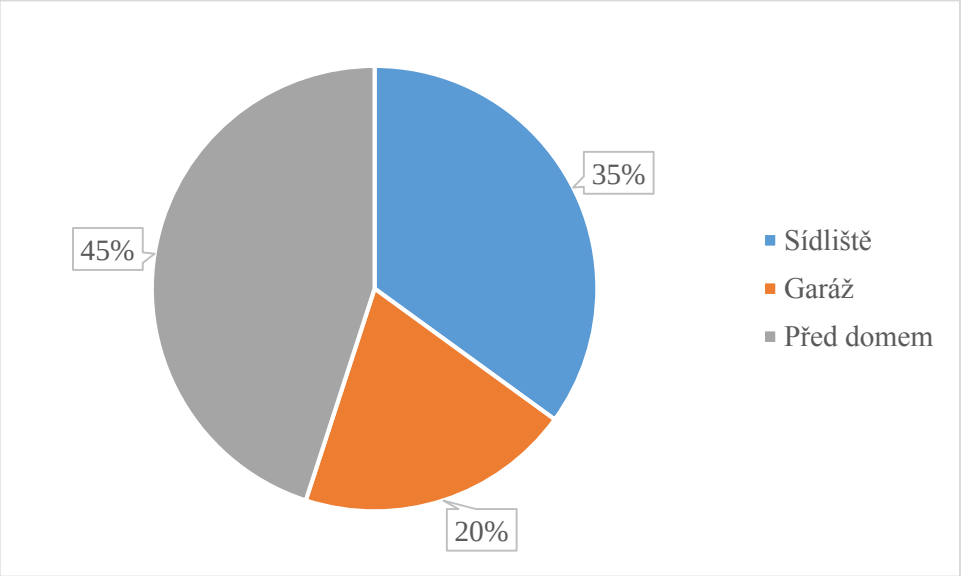
Odpovědi	Respondenti	Podíl
0 - 20 000,-	1	5%
20 000 - 60 000,-	2	10%
60 000 - 150 000,-	7	35%
150 000 - 300 000,-	7	35%
300 000,- a výš	3	15%

12) Parkujete spíše uvnitř/venku?



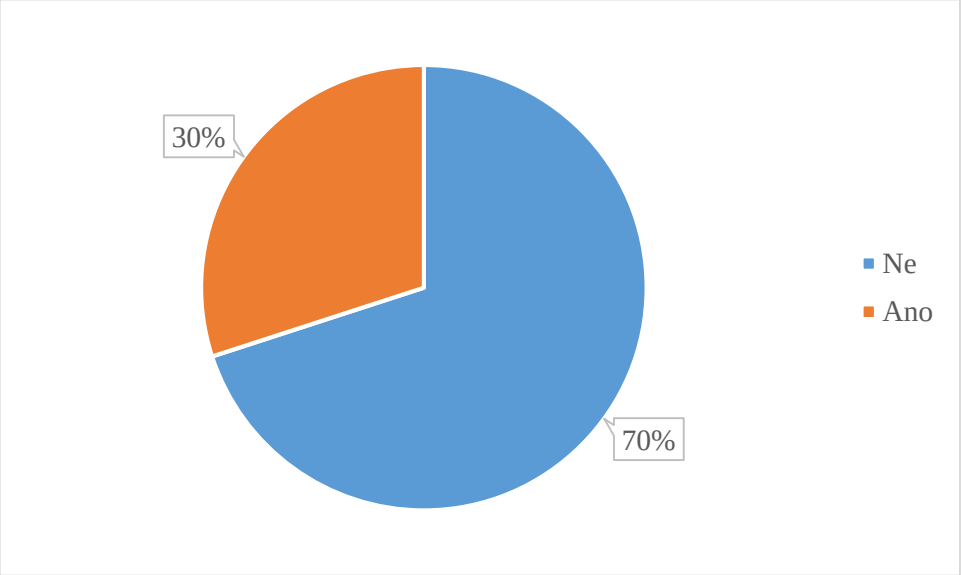
Odpovědi	Respondenti	Podíl
Uvnitř	4	20%
Venku	16	80%

13) V jaké lokalitě parkujete?



Odpovědi	Respondenti	Podíl
Sídliště	7	35%
Hlídané parkoviště	0	0 %
U obchodního centra	0	0 %
Garáž	4	20%
Před domem	9	45%
Jinde	0	0 %

14) Má dané auto nějaké zabezpečení, které není v základní výbavě auta? Pokud ano, jaké? (Zámek pedálů, volantu, GPS ...)



Odpovědi	Respondenti	Podíl
Ne	14	70%
Ano	6	30%

PŘÍLOHA P5: ROZHOVOR

1) Kde pracujete, útvar, náplň práce?

„Policie České republiky, Policejní prezídium, Úřad služby kriminální policie a vyšetřování a v současné době jsem vedoucím týmu TEMPUS, který se zabývá starými neobjasněnými vraždami se sídlem v Praze.“

2) Máte nějaký manuál k výslechům?

„Manuál samozřejmě je. Je v ní obsažená metodika výslechu, různé modelové cvičení atd. Ne na každého to platí, na výslechy se chystáme. Záleží vzhledem k tomu, jestli je to podezřelý, pachatel, svědek atd. Výslechy se chystají dopředu a dělají se vždycky takové doporučení nebo osnova, vlastně, co se hlavně tím výslechem chce zjistit.“

3) Jsou nějaké kurzy, školení ohledně výslechů v rámci policie?

„V rámci PČR musí každý kriminalista, který je oprávněn vyšetřovat trestné činy, projít kurzem. Je to vlastně operativně pátrací činnost. V tomto kurzu se učí nejen sledování a pronásledování různých osob, monitoring atd., ale učí se vlastně i výslech, tzn., jak se na ten výslech připravit, co je úkolem toho výslechu a vlastně kam ten výslech by měl směřovat. Z toho se potom skládá zkouška, která je součástí dalších kapitol, a na základě toho on dostane „oprávnění“, je to takový nejnižší stupeň, kdy může pracovat u kriminální policie.

Výslech, tam patří, jak zvládnout výslech, jak komunikovat, jak si připravit výslech, kde výslech provádět, v jakých místnostech apod. Je to součástí budoucí náplně kriminalisty. Dále se potom dají udělat samostatné kurzy, jako je výslech, jak zvládat výslechy, to jsou samostatné kurzy. Celkově je to zaměřené na ty výslechy. Jsou potom i další samostatné kurzy, jak vést tyto výslechy s pachateli nejzávažnější trestné činnosti, popřípadě výslechy mládeže, to jsou zase specializované, na každé ty osoby je to zvlášť. Ne to, co platí na mládež, tak platí na vrahy.“

Výslech tam patří, jak zvládnout výslech, jak komunikovat, jak si připravit výslech, kde výslech provádět, v jakých místnostech apod. Je to součástí budoucí náplně kriminalisty. Dále se potom dají udělat samostatné kurzy, jako je výslech, jak zvládat výslechy, to jsou samostatné kurzy. Celkově je to zaměřené na ty výslechy. Jsou potom i další samostatné kurzy, jak vést tyto výslechy s pachateli nejzávažnější trestné činnosti, popřípadě výslechy mládeže, to jsou zase specializované, na každé ty osoby je to zvlášť. Ne to co platí na mládež, tak platí na vrahy.“

4) Jaký důraz je kladen u výslechů na neverbální komunikaci v závislosti na tom, co pachatel řekne?

„Určitě, tak když ten kriminalista si ten výslech připraví a započne, tak samozřejmě v první řadě nechá toho člověka mluvit, aby řekl sám všechno. Řekne mu, proč tam je, seznámí ho s předmětem toho výslechu a důležité pro toho policistu je, aby tuto osobu nechal mluvit první sám. Potom teprve až mluví sám, klade doplňující otázky, kde se vlastně zaměří na to, co je mu známo o tom případu, jak to vypadalo na místě činu atd. Cílem je vlastně dostat podezřelou osobu do úzkých tak, aby mluvil pravdu nebo aby se k tomu přiznal. Plánuje se, kde ten výslech bude prováděn, jsou na to specializované výslechové místnosti, kde ten člověk sedí a je vyslýchán. Přes sklo ho můžou sledovat další policisté, popřípadě psycholog, psychiatr, nebo další lidé, kteří jsou zúčastnění na tom úkonu. Musí to být místnost, kde se nebude cítit pohodlně, protože pokud je podezřelý z vraždy, musí se cítit spíše takový ohrožený atd., musí si uvědomovat, co se stalo, a že tam není jenom tak, aby si popovídal s policisty. Je opravdu důležité si tyto věci nachystat.

Záznamová technika, kde ten výslech se zaznamenává, s tím souvisí. Třeba analyzátor hlasu, který potom pomůže policii ukázat, jestli je tam nějaké vnitřní chvění, zda se ten člověk cítil ohrožený nebo necítil, to se potom může nějakým způsobem zužitkovat a přenášet a využít dál. Může k té podezřelé osobě přijít policista s nabídkou fyziodetekčního vyšetření, což je tzv. detektor lži a ten vlastně pomáhá u výslechů. Nejprve se snažíme podezřelou osobu závažných skutků dostat na toto fyziodetekční vyšetření. Fyziodetekční vyšetření je pouze v Praze, dělají to tam dvě paní doktorky, je to vlastně specializovaný útvar, kde se podezřelý doveze s tím, že je to ale pouze na dobrovolnosti tady toho člověka a na základě série otázek se zjišťuje, zda ten člověk mluví pravdu nebo lže. Je to založené na tepové frekvenci, na potivosti, na citlivosti kůže atd. Po fyziodetekčním vyšetření se začnou výsledky vyhodnocovat. Potom dostaneme zprávu, kde vidíme, ve kterých otázkách ten člověk lže nebo se cítil ohrožen atd. To už se ale dělá opravdu u těch nejzávažnějších trestných činů.

U běžných trestných činů záleží na výslechových místnostech. Zvlášť se vyslýchají děti, zvlášť dospělí, popřípadě ženy atd., volíme i kdo bude přítomný u toho výslechu, jestli tam třeba budou dva nebo tři nebo tam bude nějaký specializovaný pracovník. To je třeba kapitola výslechy dětí, na to jsou dneska specializované výslechové místnosti, kde ty výslechové místnosti jsou jako dětský pokojíček, aby se to dítě cítilo dobře. Může to být dítě zneužívané nebo zneužité, nebo bylo přítomno nějakého trestného činu. Tam se snažíme navodit tu situaci, že prakticky ono neví, že se vyslýchá, jsou tam schované kamery, jsou tam kvítka, je to takové

příjemné prostředí, dítě si u toho hraje, jsou tam panenky, na kterých to dítě je schopné třeba ukázat, co mu bylo provedeno. Samozřejmě zas v takové místnosti se nemůže vyslýchat osoba podezřelá z vraždy, ty místnosti jsou strohé, je tam židle, stůl, prakticky tam nic jiného není. Je to z důvodů, aby to neupoutávalo pozornost vyslýchaného. O tom by se dalo mluvit hodiny.

Každopádně, jak jsem říkal, v první řadě se nechává člověk mluvit, řekne se mu, že je tady ve věci té a té, on by měl sám říct, jak je na té věci zúčastněn atd. a pak se snažíme dávat nějaké doplňující otázky. Samozřejmě pokud si chceme ověřit pravdivost výslechu, to potom hodně záleží na nonverbální komunikaci, kde ten policista sleduje pachatele. Spousta z nich má na to specializované kurzy, které mu pomohou rozpoznat, zda lže nebo nelže, zda tam jsou nějaké znaky úzkosti, zda hledá nějaké zastání nebo nehledá. Takže ano je to součástí, ne každý policista tuto zkušenost má, hodně s tím pracují třeba policejní vyjednavači, kteří jsou z řad policie, pak dále kriminální služba, zásahovka. Ti, co jsou z řad kriminální policie toho, využívají u výslechů, kdy oni „poznají" zda ten člověk mluví pravdu nebo ne. Jedna z variant je potom když ten vyslýchající se chce přesvědčit, zda pachatel mluví pravdu. Požádá podezřelého, aby to řekl opačně z konce dopředu, tím pádem pokud pachatel lže, málokdy je schopen to zopakovat od konce dopředu. Tady potom jde krásně vidět, zda pachatel lže nebo ne. To jsou takové praktiky, které se používají u policie ale i kdekoli jinde. Je to opravdu hodně o přípravě, vyslýchající si musí dělat poznámky atd. Priorita je nechat ho mluvit, sledovat ho, kam se dívá očima, mimiku tváře, mimiku těla, posed a všechny tyto věci se při výslechu zkoumají."

5) Nahrává se ten výslech na kameru?

„Samozřejmě se to nahrává jak který výslech, není to povinností. U závažnějších věcí, což je třeba smrt, popřípadě nějaká pedofilie na mládeži, mládeže. Tyto výslechy se nahrávají z důvodu toho, že na tu osobu nebyl činěný nějaký nátlak jak už fyzický, nebo psychický.

Potom se může záznam předložit znalci. Znalec na základě toho udělá analýzu. Protože vlastně pokud je člověk pachatelem, nebo pokud my mu prokážeme, že se dopustil vraždy, tak my ho nějakým způsobem vyslechneme, a pak mu sdělíme obvinění z trestného činu, poté má člověk nárok na obhájce a on buď potom vypovídá, nebo nevypovídá ať tak nebo tak, tak je k tomu člověku přibraný znalec, který ho vyšetří. Vyšetřuje jeho osobnost a vyšetřuje jeho osobnostní profil. Další, co vyšetřuje, je specifická věrohodnost jeho výpovědí, k tomu právě může sloužit ten záznam, na který se ten znalec podívá a na základě toho zpracuje znalecký posudek, zda ten člověk mluvil pravdu nebo nemluvil pravdu."

6) Říká vám něco jméno Paul Ekman?

„Ekman, zrovna teďka jsme o tom měli přednášku, on se zabývá mimikou tváře a vším tady tímto. Ekmanova metoda řeči těla, řeč tváře. Ale toto umí převážně už osoby, které jsou třeba v kurzu krizové komunikace, policejní vyjednavači, kdy se snažíme na základě mimiky atd. poznat tu osobu, která chce spáchat sebevraždu nebo popřípadě osobu, která drží rukojmí. Je tady několik faktorů, na které se díváme, každý může ukázat něco jiného. Ano, znám tuto metodu a využíváme ji v praxi.“

7) Je podle vás neverbální komunikace u výslechů důležitá?

„Je určitě důležitá, protože na základě toho vlastně jak znalci, tak policisté zjistí, zda jsou tam náznaky lhavosti, zda hledá nějaké zastání, zda vinu svaluje na někoho jiného, zda do toho chce zahrnout třetí osobu. Určitě se využívá často.“

8) Odhadněte, jak často pachatelé spolupracují?

„To je hrozně těžko, pachatelé spoluprací, otázkou je spíš, jaké důkazy má ta policie a podle toho se ten pachatel nebo podezřelá osoba chová. Když vidí, že z toho nevyjde dobře, tak se přizná, protože ví, že dneska přiznání je polehčující okolnost. Pokud si je jistý, že proti němu není schopen nikdo mluvit, tak samozřejmě zapírá a nechá si tu věc dokázat, protože z jeho pohledu je možná nejsnadnější v tu chvíli odmítnout vypovědět. Až mu policie sdělí obvinění, až ukáže ty trumfy, co proti němu má, tak teprve potom začne buď spolupracovat, nebo nezačne. Tam záleží, i jakého má advokáta, těch faktorů je tam víc, vesměs spolupracují pachatelé, kteří nejsou tak kriminálně zdatní, kdy třeba způsobil vraždu a ta pramenila z nevyrovnaných vztahů s manželkou. Nejsou to otřelí kriminálnicí. Co se týče otřelých kriminálníků, tak ti většinou spolupracují tehdy, když vidí, že se z toho nedostanou. Ví, že spoluprací si potom jede o trest a o všechno, může to zúročit u soudu, dostane nižší trest, nižší skupinu ve vězení s menší ostrahou atd.“

9) Jak často pachatelé lžou, v porovnání neverbální komunikace s důkazy?

„Na toto moc nejde odpovědět, kdy pachatelé lžou, to opravdu závisí na těch důkazech. Když je ten člověk chycený na místě činu, tak málo kdy řekne, že šel náhodou kolem … Samozřejmě je tam jejich DNA, jsou tam daktyloskopické stopy, pachové stopy a další tady tyto věci, i věk tady hraje roli. Takoví otřelí kriminálníci, ti vyloženě řeknou „pane Baláž však to víte, já se s vámi bavit nebudu, dokažte mi to“ apod. Lžou, zkouší to ze začátku vesměs všichni, ale oni poznají, jestli ta policie na ně něco má, nebo nemá. Potom spíše odmítnou vypovídat. Nechají, ať jim to policie prokáže.“

10) Myslíte si, že analýza neverbální komunikace, prvky sociálního inženýrství jsou důležité pro PKB?

„Na to se policisté připravují, například při modelových situací. Dá se nachystat na spoustu věcí, ale prostě ve finále, i ze strany policejního vyjednavače můžu říct, že jsme byli připraveni na cokoli, že budeme vyjednávat se sebevrahy, s únosci, všechno toto se stalo, ale ve finále je to všechno úplně jinak. Člověk zažívá takový ten adrenalin, zodpovědnost atd.“

11) Setkal jste se se sociálním inženýrstvím

„Toto není až tak pojem pro kriminalistu nebo pro policistu, toto je spíše takový pojem celkový. Třeba u policie se hodně používá krizová komunikace, toto všechno je zaměřeno na naši práci. Potom dále operativní vytěžování, operativní šetření, výslechy, různé kriminalistické verze atd. Minimum tady s tím sociálním inženýrstvím.“

12) Obsahuje manuál prvky soc. inženýrství?

„To se vyučuje hodně v psychologii, ale říkám je to hodně specifické. Co se týče policie, je to hrozně zaměřené na tu policejní činnost. Každý ten budoucí policista má možnost si zvolit specifické předměty jako kriminalistka, kriminologie, všechno je spíše zaměřené na tu policejní činnost.“