UNIVERZITA PARDUBICE

FAKULTA EKONOMICKO-SPRÁVNÍ

BAKALÁŘSKÁ PRÁCE

2023 Tomáš Pištělák

Univerzita Pardubice

Fakulta ekonomicko-správní

Digitální důvěra

Tomáš Pištělák

Bakalářská práce

2023

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2022/2023

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Tomáš Pištělák**
Osobní číslo:	**E20146**
Studijní program:	**B0688A140004 Informatika a systémové inženýrství**
Specializace:	**Informatika ve veřejné správě**
Téma práce:	**Digitální důvěra**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování

Cílem práce je charakterizovat aspekty digitální důvěry. Práce bude zaměřena jak na hledisko technické, tak na přístup a vnímání uživatelů různých digitálních úkonů. Součástí bude dotazníkové šetření s tématikou povědomí o prvcích digitální důvěry mezi studenty univerzity.

Osnova:
- Základní pojmy související se zpracovávanou problematikou.
- Charakteristika vybraných aspektů.
- Dotazníkové šetření.

Rozsah pracovní zprávy: **cca 35 stran**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

DOUCEK, Petr, Martin KONEČNÝ a Luděk NOVÁK. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.
LECHNER, Tomáš. *Elektronické dokumenty v právní praxi*. Praha: Leges, 2013. Praktik. ISBN 978-80-87576-41-0.
PAVLÍK, Marek, Karel ŠIMKA, Josef POSTRÁNECKÝ a Richard POMAHAČ. *Moderní veřejná správa: zvyšování kvality veřejné správy, dobrá praxe a trendy*. Praha: Wolters Kluwer, 2020. ISBN 978-80-7598-048-9.
VEBER, Jaromír. *Digitalizace ekonomiky a společnosti: výhody, rizika, příležitosti*. Praha: Management Press, 2018. ISBN 978-80-7261-554-4.

Vedoucí bakalářské práce: **doc. Ing. Stanislava Šimonová, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **1. září 2022**
Termín odevzdání bakalářské práce: **30. dubna 2023**

L.S.

prof. Ing. Jan Stejskal, Ph.D. v.r.
děkan

RNDr. Ing. Oldřich Horák, Ph.D. v.r.
vedoucí ústavu

V Pardubicích dne 1. září 2022

Prohlašuji:

Práci s názvem „Digitální důvěra” jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury. Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 9. 12. 2023

Tomáš Pištělák

PODĚKOVÁNÍ

Na tomto místě bych rád upřímně poděkoval doc. Ing. Stanislavě Šimonové, Ph.D., vedoucí mé bakalářské práce, za odborné vedení při zpracování práce, trpělivost, ochotu pomoci a cenné rady. Dále bych chtěl poděkovat své rodině za podporu v celém průběhu studia, bez níž by tohoto milníku nebylo možno dosáhnout. Na závěr bych chtěl poděkovat všem kamarádům, kteří mi dokázali pomoci vždy, když jsem si nevěděl rady a s kterými jsem mohl sdílet pravděpodobně poslední kapitolu svého studentského života. Děkuji!

ANOTACE

V kontextu rychle se rozvíjejících digitálních technologií a interakcí se bakalářská práce zaměřuje na digitální důvěru v současném digitálním prostředí. Práce zkoumá vybrané aspekty tohoto pojmu a využívá dotazníkového šetření mezi studenty. Cílem šetření je získání jejich názorů na digitální důvěru a jednotlivé prvky s tímto konceptem spojené.

KLÍČOVÁ SLOVA

Důvěra, digitální důvěra, digitální identifikační doklady, eDoklady, umělá inteligence, elektronický podpis

TITLE

Digital trust

ANNOTATION

In the context of rapidly evolving digital technologies and interactions, the bachelor's thesis focuses on digital trust in the current digital environment. The thesis examines selected aspects of this concept and utilizes a questionnaire survey among students. The aim of the survey is to gather their opinions on digital trust and its associated elements.

KEYWORDS

Trust, digital trust, digital identification documents, eDoklady, artificial intelligence, electronic signature

OBSAH

Úvod 12

1. Vymezení tématu bakalářské práce 13

1.1 Návrh postupu zpracování 13

1.2 Vymezení aspektů 14

1.3 Zkoumání jednotlivých aspektů 15

2. Důvěra 15

2.1 Definice důvěry 15

2.2 Nástroje k získání důvěry 16

3. Fyzická důvěra v digitálním světě 17

3.1 Důsledky digitalizace dokladů 18

3.2 Výhody digitalizace dokladů 19

3.3 Nevýhody digitalizace dokladů 20

3.4 Shrnutí 21

4. Digitální důvěra 21

4.1 Digitální důvěru staví organizace 24

4.1.1 Pilíř 1: Transparentnost a dostupnost 24

4.1.2 Pilíř 2: Etika a zodpovědnost 25

4.1.3 Pilíř 3: Soukromí a kontrola 26

4.1.4 Pilíř 4: Bezpečnost a spolehlivost 26

4.2 Přínosy a nevýhody 27

4.3 Faktory ohrožující digitální důvěru 30

4.4 Shrnutí 30

5. Bezpečnost a zvyšování digitální důvěry 31

5.1 Elektronický podpis, pečeť a razítko 31

5.1.1 Kvalifikovaný elektronický podpis 32

5.1.2 Zaručený elektronický podpis založený na kvalifikovaném certifikátu ... 32
5.1.3 Zaručený elektronický podpis ... 32
5.2 Elektronická pečeť a razítko ... 32
5.3 Vícefaktorová autentizace ... 33
5.4 Shrnutí ... 34
6. Umělá inteligence ... 35
6.1 Metody umělé inteligence ... 36
6.2 Deepfake a dezinformace ... 37
7. Dotazník ... 39
7.1 Prvky digitální důvěry ... 41
7.2 Výzkumný problém ... 41
7.3 Analýza dotazníku ... 41
7.4 Analýza jednotlivých odpovědí ... 41
7.5 Test nezávislosti ... 53
7.5.1 Test nezávislosti mezi otázkou 2 a 3 ... 54
7.5.2 Test nezávislosti mezi pohlavím a otázkou 10 ... 56
7.6 Vyhodnocení dotazníku ... 58
7.7 Zhodnocení výzkumu ... 60
Závěr ... 61
Použitá literatura ... 63
Přílohy ... 68

SEZNAM OBRÁZKŮ

Obrázek 1: Systém práce 13
Obrázek 2: Myšlenková mapa 14
Obrázek 3: Aplikace eDoklady 18
Obrázek 4: Microsoft Authenticator 34
Obrázek 5: Deepfake 38
Obrázek 6: Popis ChatGPT 38
Obrázek 7: ChatGPT – vytvoření textu 39
Obrázek 8: Chí-kvadrát vzorec 53
Obrázek 9: Kontingenční tabulka 54
Obrázek 10: Očekávané četnosti 55
Obrázek 11: Výpočet hodnoty testovací statistiky 55
Obrázek 12: Výsledek testu nezávislosti mezi otázkou 2 a 3 56
Obrázek 13: Skutečné a očekávané četnosti 57
Obrázek 14: Výsledek testu nezávislosti mezi pohlavím a otázkou 10 57

SEZNAM GRAFŮ

Graf 1: Otázka 3 – Uvažování o používání aplikace 44
Graf 2: Otázka 4 - Bezpečnost identifikačních dokladů 45
Graf 3: Otázka 5 - Zneužití osobních informací 45
Graf 4: Otázka 6 - Reakce na únik dat z organizace 46
Graf 5: Otázka 7 – Využití bezhotovostních plateb 47
Graf 6: Otázka 8 - Bezpečnost bezhotovostních plateb 48
Graf 7: Otázka 9 – Využívání elektronického podpisu 48
Graf 8: Otázka 10 - Využívání vícefaktorového ověření 49
Graf 9: Otázka 11 - Preference online řešení záležitosti nebo osobní kontakt 50
Graf 10: Otázka 12 - Preference elektronických zdrojů nebo tištěných 51
Graf 11: Otázka 13 - Obavy z hlediska falešnosti informací v digitální formě 51
Graf 12: Otázka 14 - Vnímání trendu implementace umělé inteligence 52
Graf 13: Otázka 15 – Obavy z využívání umělé inteligence k šíření dezinformací 53

SEZNAM TABULEK

Tabulka 1: Studijní program a pohlaví 42
Tabulka 2: Procentuální zastoupení fakult 42

SEZNAM ZKRATEK A ZNAČEK

AI	Artificial Intelligence
UPCE	Univerzita Pardubice
GDPR	General Data Protection Regulation
eIDAS	Electronic identification and trust services
ČR	Česká republika
GPS	Global positioning systém
EU	Evropská Unie

Úvod

Rozvoj digitálních technologií a rostoucí digitalizace společnosti mění způsob chápání důvěry v digitálním světě. Termín „digitální důvěra“ získává na významu z hlediska rostoucích digitálních interakcí a využívání nových technologií. Tento rozvoj ovlivňuje vytváření a údržbu důvěry v digitálním prostředí.

Cílem práce je charakterizovat aspekty digitální důvěry. Práce bude zaměřena jak na hledisko technické, tak na přístup a vnímání uživatelů různých digitálních úkonů. Součástí bude dotazníkové šetření s tématikou povědomí o prvcích digitální důvěry mezi studenty univerzity.

Digitální důvěra představuje komplexní koncept, proto jsem se rozhodl v úvodní části práce konkrétně vymezit aspekty, na něž se zaměřím. Byly vybrány aspekty, které jsou v dnešní době nejen důležité, ale také již ovlivňují, a z hlediska rozvoje digitálních technologií budou ovlivňovat, život z pozitivního i negativního hlediska.

Vybrané aspekty byly zkoumány v další části práce. Předchozí zkoumání charakteristik jednotlivých aspektů digitální důvěry se stalo zdrojem pro selekci prvků, jenž by byly relevantní i pro využití v otázkách dotazníku.

Poslední část bakalářské práce spočívala ve vytvoření dotazníkového průzkumu. Dotazník byl speciálně určen pro studenty UPCE, jež představují mladší věkovou skupinu respondentů. Otázky se zaměřují na názory a preference v různých aspektech digitální důvěry. Kromě zjištění, co si představují pod pojmem „digitální důvěra,“ bylo nadále zkoumáno, jaké mají mínění o vybraných prvcích spojených s důvěrou v digitálním prostředí. Výsledky poslouží ke zjištění názorů na dané prvky digitální důvěry.

1. Vymezení tématu bakalářské práce

V této kapitole specifikuji můj plánovaný postup práce směřující k naplnění stanoveného cíle.

1.1 Návrh postupu zpracování

Cíle práce bude dosaženo v etapách:

A. **Vymezení aspektů:** Digitální důvěra je rozsáhlý koncept, proto je první krok zaměřen na výběr konkrétních aspektů, kterým se má práce bude věnovat.

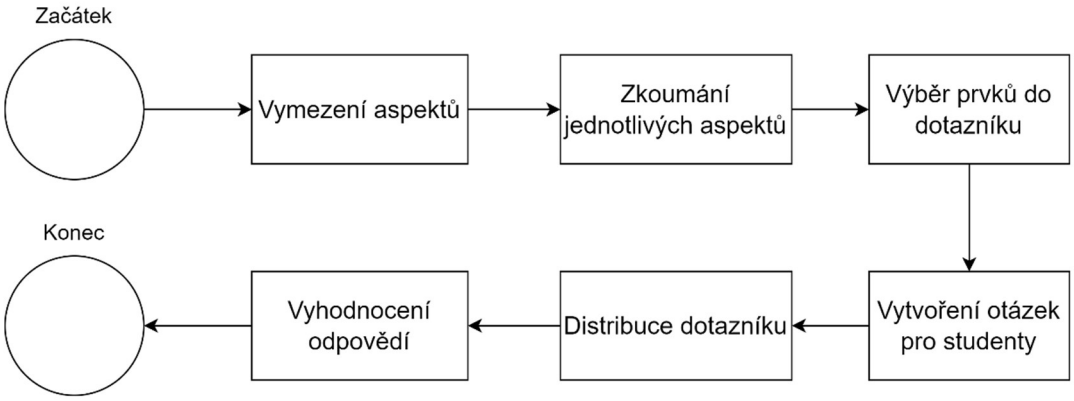
B. **Zkoumání jednotlivých aspektů:** Na základě internetových zdrojů a literatury budou zkoumány jednotlivé aspekty.

C. **Výběr prvků do dotazníku:** Na základě předešlého zkoumání budou identifikovány relevantní prvky pro začlenění do dotazníku.

D. **Vytvoření otázek pro studenty:** V této etapě budou vytvořeny relevantní otázky pro studenty obsahující prvky vybrané v předešlém kroku. Každý ze studentů vyplňujících můj dotazník může mít k tomuto tématu jiný přístup a také jiné vnímání digitálních úkonů, čímž bude prakticky zaručena jistá rozdílnost názorů na mé otázky.

E. Distribuce dotazníku: Zahrnuje rozeslání dotazníku studentům UPCE a shromáždění jejich odpovědí.

F. Vyhodnocení odpovědí: Po obdržení odpovědí bude provedena analýza a vyhodnocení těchto dat.

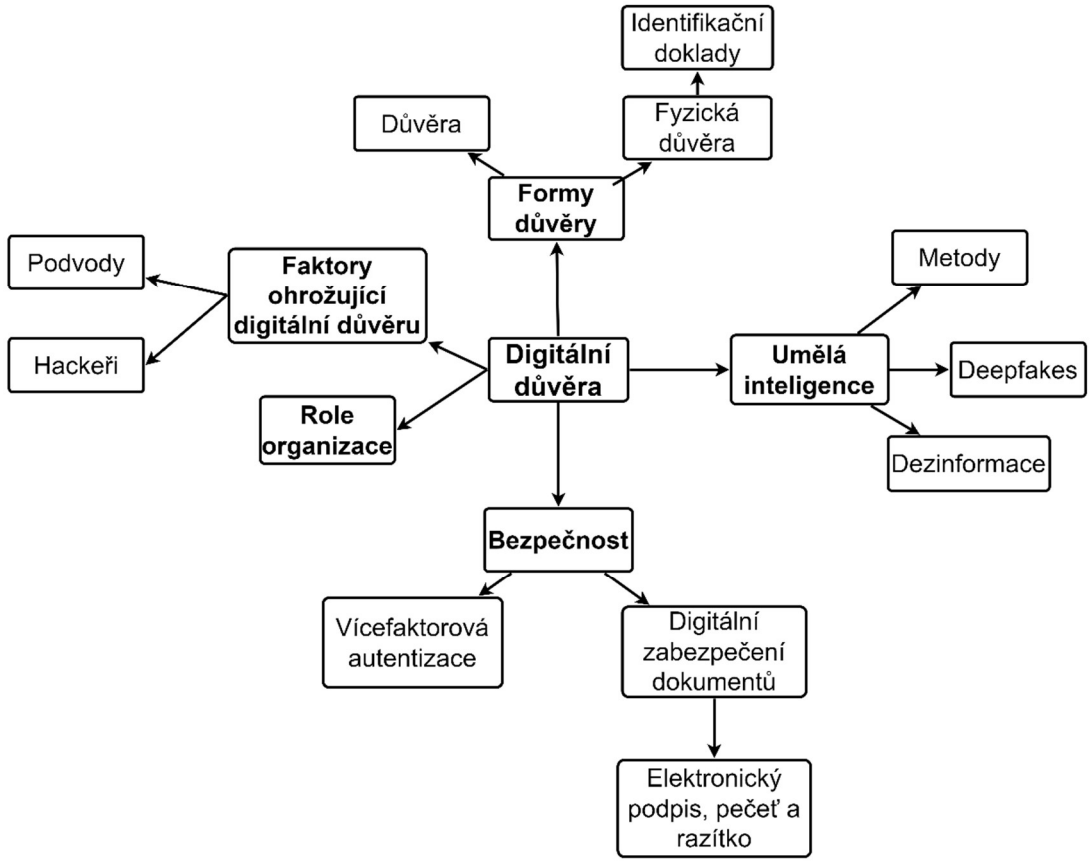


Obrázek 1: Systém práce

Zdroj: Vlastní zpracování

1.2 Vymezení aspektů

Pro vymezení aspektů jsem vytvořil myšlenkovou mapu, viz Obrázek 2



Obrázek 2: Myšlenková mapa

Zdroj: Vlastní zpracování

V mé práci bude vysvětlen a používán pojem "důvěra" jako kontrast k pojmu "digitální důvěra." Oba pojmy obsahují lišící se charakteristiky. Spojitost s digitální důvěrou má i fyzická důvěra, představující důvěru ve fyzické prvky, zde konkrétně v identifikační doklady. Dalším aspektem bude zkoumání role organizací z hlediska jejich vlivu na budování a udržování digitální důvěry. Práce se taktéž zaměří na faktory, které mohou ohrozit digitální důvěru, specificky na hackery a podvody v online světě.

Z technického hlediska bude probrán aspekt bezpečnosti, který se bude věnovat vícefaktorové autentizaci, představující důležitý prvek ochrany digitálních účtů. Dalším prvkem bude digitální zabezpečení dokumentů jednotlivými technikami pro zajištění věrohodnosti elektronických dokumentů.

Nakonec se zaměřím na téma umělé inteligence, kde budou popsány metody a využívání umělé inteligence v tvorbě deepfakes a dezinformací.

1.3 Zkoumání jednotlivých aspektů

Na základě internetových zdrojů a literatury budou zkoumány jednotlivé aspekty. Následující oblasti jsem zvolil jako hlavní, jelikož zastřešují všechny aspekty:

- Důvěra
- Fyzická důvěra v digitálním světě
- Digitální důvěra
- Bezpečnost a zvyšování digitální důvěry
- Umělá inteligence

2. Důvěra

Digitální důvěra se v několika důležitých věcech liší od důvěry obecné, ale obsahuje většinu jejích hlavních charakteristik. Proto se práce tématem důvěry bude zabývat podrobněji. Na termín důvěra vzniklo obrovské množství definicí a často se od sebe liší. Rozmanitost těchto definicí může způsobovat nesrozumitelnost při snaze určit, která z nich nejlépe a nejpřesněji vystihuje pojem důvěra. S tím, že mnoho autorů definovalo důvěru jiným způsobem, se dá poukázat na to, že je obtížné přesně definovat tento pojem. [1]

2.1 Definice důvěry

Na termín důvěra jsou různé pohledy:

- Bernard Barber definoval důvěru, jako soubor „*sociálně naučených a sociálně potvrzených očekávání, která mají jeden od druhého, od organizací a institucí, ve kterých žijí a od přirozených a morálních společenských řádů, které určují základní chápaní jejich životů.*“ [2]
- Druhá definice: „*Důvěru definujeme jako sebevědomá pozitivní očekávání ohledně chování druhého*“. [2]
- Třetí definice: „*Psychologický stav zahrnující záměr přijmout zranitelnost na základě pozitivních očekávaných záměrů nebo chování druhého*“. [3]

Obecně napříč obory panuje shoda na podmínkách pro vznik důvěry. Jednou z hlavních podmínek je riziko, které se musí podstoupit. Spojení mezi důvěrou a riskováním má vzájemný vztah – riziko vytváří příležitost pro důvěru, která vede k riskování. Podstupování rizika navíc posiluje pocit důvěry, když se očekávané chování naplní. Druhou nutnou podmínkou důvěry je vzájemná závislost, kdy nelze dosáhnout zájmů jedné strany bez spoléhání se na stranu druhou. Povaha rizika

a důvěry se s rostoucí vzájemnou závislostí mění. Stupně vzájemné závislosti ve skutečnosti mění formu, kterou může důvěra nabývat. [4]

V častých případech nemůže být vkládána plná důvěra, a tím pádem podstupováno dané riziko. Například služby veřejné správy, policie, banky atd. nemohou vložit důvěru v osoby, jejichž identita nebyla předem řádně ověřena. Musely být vyvinuty takové nástroje, jež umožní tuto důvěru v daných situacích vytvořit.

2.2 Nástroje k získání důvěry

Při vyřizování půjčky, či vyřizování záležitostí na úřadě, musí být prokázána totožnost, pro odstranění pochyb o tom, že osoba vystupující, je opravdu ta osoba, za kterou se vydává. Osoba tedy musí vložit plnou důvěru dané osobě/instituci, že soukromé údaje nijak nevyužije v její neprospěch.

Nejčastějším způsobem, jak může osoba prokázat svou totožnost, je formou občanského průkazu, který je povinen mít každý občan ČR od dovršení věku 15 let a mající trvalý pobyt na území ČR. Popřípadě lze občanský průkaz na žádost vydat i občanovi mladšímu 15 let, i občanovi bez trvalého pobytu na území ČR. [5] Dalším běžným postupem pro ověření totožnosti může být použití cestovního pasu nebo řidičského průkazu jako prostředku identifikace.

Nicméně, v dnešní době je možné i tuto možnost prokázaní totožnosti zfalšovat. Na černém internetovém trhu je možné koupit falešné doklady, jejichž cena se odvíjí od druhu, úrovně zpracování nebo země původu. Tuzemské doklady patří k těm nejdražším. Podle analýzy společnosti NordVPN český cestovní pas stojí 92 000 Kč, občanský průkaz 28 000 Kč a řidičský průkaz stejně tak. Pachatelé tyto dokumenty používají k prokazování se na ulici, k vyřízení půjčky a k dalším činnostem. Zatím není možnost i v tomto hledat jistotu, tedy mít naprostou důvěru, že osoba je tou osobou, za kterou se vydává. Odrazující nemusí být ani vysoké tresty za padělání, či užívání padělaných dokladů, kdy pachatelé mohou jít do vězení až na deset let. [6]

Falešný cestovní pas nebo občanský průkaz pachatelé těžko použijí pro cestování. Cestovní pas a od 2. srpna 2021 i občanský průkaz disponují strojově čitelnými údaji a nosičem dat s biometrickými údaji. [5] [7]

Může být konstatováno, že zatím není možné dosáhnout naprosté důvěry v nástroje ve fyzické podobě, které by dokázaly pochyby zcela odstranit. V souvislosti s tím, jak se společnost posunuje vpřed, tak nastává doba, kdy se moderní technologie stávají

neodmyslitelnou součástí lidských životů. To zahrnuje i digitalizaci fyzických prvků, jako je občanský průkaz.

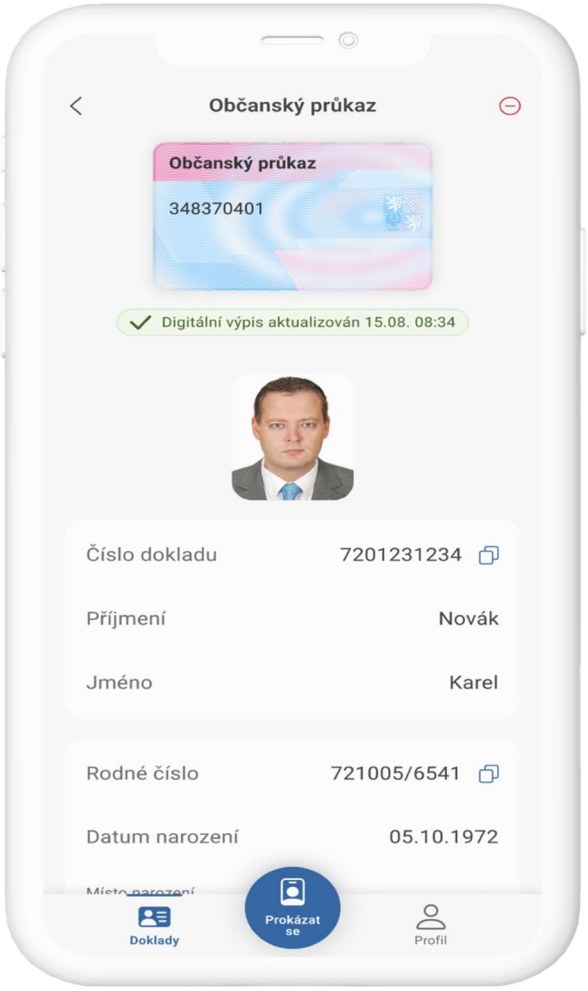
3. Fyzická důvěra v digitálním světě

Digitalizace postupně odsouvá fyzické prvky do pozadí, neboť nabízí možnost mít veškeré důležité informace a prvky, které byly dříve dostupné pouze ve fyzické podobě, uložené v digitální podobě. Mobilní telefon se stal v tomto směru klíčovým nástrojem, který lidi provází na každém kroku a umožňuje mít prakticky všechny důležité informace na dosah ruky. Tato digitalizace by mohla být obzvláště přínosná pro mladší generaci vyrůstající v době, kdy mobilní telefony jsou nedílnou součástí jejich života a jejich používání se stalo samozřejmostí již od jejich raného věku.

V programovém prohlášení vlády, kdy jeho upravenou podobu schválil kabinet na jednání 1. března 2023, existuje bod v tématu „Digitalizace“, jehož náplní je: „*Co nejrychleji, nejpozději v roce 2023, zrušíme povinnosti nosit u sebe průkazy a dokumenty, pokud si je stát může ověřit jinak (tvorba tzv. eDokladovky), kompatibilní s elektronickými doklady EU.“* [8] Tato aktivita navazuje na nařízení evropského parlamentu a rady, které mění nařízení (EU) č. 910/2014. Nařízení je známe též jako eIDAS 2.0 a představuje klíčovou legislativní iniciativu EU zaměřenou na posílení bezpečnosti elektronických transakcí a digitalizaci identifikačních prostředků v rámci celé Evropské unie. V rámci nového nařízení je zde důležitým prvkem evropská peněženka digitální identity. Tato peněženka by měla sloužit jako centralizované úložiště pro různé typy elektronických identifikačních prostředků. V platnost vejde v roce 2025. [8] [9]

Toto nařízení je platné pro všech 27 členských států v Evropské unii. Počítá se s tím, že každý stát bude mít vlastní systém digitalizace identifikačních prvků propojený na evropské úrovni. Každý člen bude muset podniknout nezbytné kroky, směřující k naplnění tohoto cíle, včetně České republiky. V rámci splnění tohoto cíle se vytvořila aplikace eDoklady, kterou si uživatel bude moci nainstalovat do svého mobilního telefonu nebo jiného mobilního zařízení od ledna roku 2024. Tato aplikace reaguje na rostoucí potřebu digitalizace identifikačních prvků. Do této aplikace se budou moct nahrávat jednotlivé identifikační doklady aktuálně dostupné ve fyzické podobě, které občanům vydává stát. Pro občany bude pro využívání této aplikace nezbytnou podmínkou vlastnictví chytrého telefonu a vytvořená Identita občana. Jedná se pouze

o doplnění k fyzickým dokladům. [10] Na obrázku je vidět, jak tato aplikace vypadá z pohledu osoby.



Obrázek 3: Aplikace eDoklady

Zdroj: https://edoklady.gov.cz

3.1 Důsledky digitalizace dokladů

Digitalizace identifikačních prvků přináší nejen technologické změny, ale také mění způsob, jakým společnost bude vnímat a používat identitu. Fyzické identifikační průkazy byly vyžadovány při interakci s institucemi nebo při ověřování totožnosti. S nástupem digitálních identifikačních prvků se možnosti využití rozšiřují a zjednodušují použití v digitálním prostředí. U obou typů nastává otázka z hlediska bezpečnosti. Zatímco problémem u fyzických průkazů je jejich ztráta nebo falšování. U jejich digitální podoby je klíčovým hlediskem bezpečnost digitálních systémů a ochrana před kybernetickými hrozbami. Ztráta mobilního telefonu nemusí být tak vážným problémem v porovnání se ztrátou fyzického průkazu, například občanského nebo řidičského. Samotné mobilní telefony mohou být zabezpečeny pomocí hesla

nebo dalších autentizačních metod, jako je biometrické zabezpečení, či PIN. Dalším ochranným prvkem bude zabezpečený přístup do aplikace eDoklady, kde jsou identifikační doklady uloženy, což dále zvětšuje bezpečnost těchto informací. Falešné fyzické průkazy mohou být vytvářeny tak precizně, že je obtížné je odhalit pouhým okem. Digitalizace by měla snížit počet případů jejich zfalšování. Aplikace eDoklady se pyšní tím, že nebude možné doklad zfalšovat a vydávat se za někoho jiného. Ověřovatel musí rozšifrovat zašifrované údaje a tím se ověří jejich platnost. [10]

3.2 Výhody digitalizace dokladů

Digitalizace identifikačních dokladů bude mít několik hlavních výhod pro uživatele. V této práci se zaměřím na aplikaci eDoklady.

Jedná se o tyto výhody:

- V budoucnu centralizace dokladů do jedné aplikace
- Významné eliminování možnosti ztráty dokladů
- Eliminace falšování dokladů
- Zabezpečení

Aplikace eDoklady bude mít v budoucnu možnost spravovat více dokladů, což uživatelům přinese mnohé výhody a usnadní jim řadu situací. To znamená, že člověk s nainstalovanou aplikací, importovaným dokladem a Identitou občana nebude muset s sebou nosit fyzické průkazy.

Spravování více dokladů v jedné aplikaci může pomoci významně eliminovat možnost ztráty dokladů. Je to z těchto důvodů:

- Všechny důležité a podporované průkazy budou na jednom místě, což zamezuje ztrátám jednotlivých průkazů.
- Nepotřeba nosit několik fyzických průkazů

Centralizací osobních dokladů do jedné aplikace se nejen sníží počet jejich zneužití, díky zabezpečení mobilního telefonu heslem, či jiným prvkem, ale také se výrazně zvýší zabezpečení těchto dokladů. Taktéž přístup do aplikace bude zajištěn na bázi autentizace, kdy se biometrií zajistí přihlášení do aplikace a při případném selhání biometrie se použije přihlašovací PIN. Při ztrátě telefonu půjde v Portálu občana aplikaci eDoklady odpojit. [10]

Soukromí poskytovatelé služeb využívající infrastrukturu eIDAS budou moci poskytovat přístup k potencionálním zákazníkům v jiných členských státech Evropské

unie. Možnost poskytnutí těchto služeb spočívá v tom, že umožní zahraničním občanům EU používat svou národní identitu k přístupu k jejich službám. [11]

Bezpečnost je regulována v rámci eIDAS, kde je kladen důraz na vysokou úroveň zabezpečení a tím se snižuje riziko krádeže identity a zneužití osobních údajů. Provedené transakce mají stejnou právní platnost jako tradiční papírové procesy, čímž je zajištěna jejich důvěryhodnost a právní závaznost. [11]

3.3 Nevýhody digitalizace dokladů

Používání osobních dokladů v digitální podobě má mnoho výhod, ale také nese nevýhody, které je nutné zvážit. Ačkoliv nelze eliminovat všechny tyto nevýhody, v průběhu nastupující éry digitalizace budou minimalizovány díky lepší informační gramotnosti. Z tohoto důvodu důvěra v digitální podobu osobních dokladů vzroste, což povede ke zvýšení jejich využívání.

Nevýhody ovlivňující používání osobních dokladů v digitální podobě:

- Technologické limitace
- Vyloučení skupin obyvatelstva
- Potřeba informační gramotnosti
- Zranitelnost vůči kybernetickým hrozbám
- Technické problémy a nedostupnost

Mohou existovat technologické limitace, kdy někteří jedinci mají mobilní telefon s nedostačujícími specifikacemi, popřípadě vůbec nemají mobilní telefon nebo jiné vhodné zařízení, na kterém by mohli mít aplikaci nainstalovanou, což brání jejich přístupu do tohoto nástroje, a tedy i jeho používání. Tato nevýhoda je spojena s další nevýhodou, kterou představuje vyloučení určitých skupin obyvatelstva. Jedná se o skupinu obyvatelstva, jež není dobře obeznámena s moderními technologiemi nebo jsou skeptičtí a nedůvěřiví vůči novým technologiím. Pro odstranění, či alespoň zmenšení nedůvěry v digitalizaci osobních dokladů je potřeba dostatečná úroveň informační gramotnosti. Tato znalost pomáhá uživatelům lépe porozumět výhodám, ale také existujícím rizikům. Díky tomu mohou uživatelé racionálně zvážit, zda chtějí tuto aplikaci používat a zda z ní budou mít přínos.

Osobní údaje uložené v digitálním formátu podléhají riziku zranitelnosti vůči kybernetickým hrozbám. To znamená, že základní problém tvoří hackeři nebo jiné osoby s úmyslem narušit bezpečnost systému. Tímto způsobem by mohly být odhaleny potenciálně citlivé údaje osoby.

Opakované technické problémy a nedostupnost mohou být frustrujícím faktorem. Pokud by tyto problémy přetrvávaly nebo se vyskytovaly opakovaně, mohlo by dojít ke ztrátě smyslu používání aplikace namísto fyzického osobního dokladu, čímž by se znehodnotily výhody, které by digitalizace měla přinést. [12]

3.4 Shrnutí

Osobní průkazy v digitální podobě nabízejí řadu výhod, ale nesou i nevýhody. Mezi výhody patří efektivita a pohodlí pro uživatele, protože může mít veškeré důležité podporované osobní průkazy umístěné na jednom místě. Mezi nevýhody se může zahrnout technologická limitace, technické problémy, nedostupnost a zranitelnost vůči kybernetickým hrozbám. Další nevýhodou, jsou cílení potencionální uživatelé, kdy se vyloučí skupina obyvatelstva, která nemá dostatečné prostředky, nebo neoplývá informační gramotností.

Zde se začíná odlišovat důvěra ve fyzické doklady od důvěry v jejich digitální formu. Přechod na digitální podobu osobních dokladů přináší nové úvahy, které se týkají způsobu, jak je lidmi důvěřována a vnímána. Dosavadní důvěra ve fyzické průkazy byla založena na jejich hmatatelnosti. S přechodem na digitální podobu bude důvěra založena převážně na technologii a systémech. To může vyvolávat obavy ohledně bezpečnosti a ochrany osobních údajů. Tento vývoj v rámci důvěry otevírá nový prostor pro koncept digitální důvěry, postupně nabývající na významu. V současné době je stále více aspektů přesouváno nebo nově vytvářeno v digitálním prostoru. Digitalizace osobních dokladů je pouze jedním z mnoha příkladů této transformace, kdy dokonce i základní prvek identifikace bude možné využívat v digitální formě. S rostoucím vlivem digitálních technologií a služeb se také zvyšuje důležitost a potřeba digitální důvěry.

4. Digitální důvěra

Podle statistiky vytvořené v dubnu roku 2023 bylo zjištěno, že v celosvětovém měřítku existuje přes 5 miliard uživatelů internetu, což představuje přes 64 procent celosvětové populace planety. [13] Tento fakt naznačuje, že digitální technologie mají významný vliv na současnou společnost a taktéž poukazuje na to, že moderní technologie začínají být neodmyslitelnou součástí našich životů, kdy i fyzické prvky se přesouvají do digitální podoby. Probíhající vývoj vytyčuje rostoucí éru digitalizace a s ní související zvýšené využití digitálních technologií. Tímto se také mění způsob vnímání a vkládání

důvěry v digitální prostředky. Paralelně s tím vznikají nové hrozby a rizika, které mohou narušit formující se digitální důvěru.

Pojem digitální důvěra nedisponuje obecně uznávanou definicí. V online světě lze na toto téma nalézt několik navzájem se podobajících názorů. Na základě mého zkoumání jsem vybral tři různé perspektivy na termín digitální důvěra, prezentované s odlišnými formulacemi.

1. Digitální důvěra je očekávání jednotlivců, že digitální technologie a služby – a organizace je poskytující – budou chránit zájmy všech zúčastněných stran a dodržovat společenská očekávání a hodnoty. [14]
2. Digitální důvěra se týká implicitní důvěry, kterou jednotlivci a organizace vkládají do správců svých důvěrných údajů během online transakcí. Jedná se o záruku, že data budou zpracována podle dohodnutých podmínek, chráněna před zneužitím a že bude zajištěna jejich bezpečnost v digitálním prostoru. [15]
3. Digitální důvěra znamená důvěru uživatelů v schopnost lidí, technologií a procesů vytvořit bezpečný digitální svět. Digitální důvěra je udělována společnostem, které uživatelům ukázaly, že dokážou poskytovat bezpečnost, soukromí, spolehlivost a etiku dat prostřednictvím svých online programů nebo zařízení. [16]

První perspektiva se v zásadě vztahuje k tomu, že digitální technologie a služby, které poskytují organizace, budou použity zodpovědným a etickým způsobem. Organizace, jež tyto služby poskytují, budou jednat v nejlepším zájmu celé společnosti, což znamená, že vývoj a nasazení digitálních technologií budou prospěšné pro všechny a nevyvolají negativní dopady.

Druhý pohled na digitální důvěru se zaměřuje na klíčový aspekt – implicitní důvěra. Tento koncept zahrnuje automatické vkládání důvěry do správců svých důvěrných údajů, kterými mohou být jednotlivci i organizace. Těmto entitám je svěřena odpovědnost za ochranu osobních dat a zajištění jejich bezpečnosti. Implicitní důvěra zde vyzdvihuje zahrnutou podstatu očekávání, že správci budou jednat zodpovědně.

Kontext třetího pohledu na digitální důvěru pojednává o důvěře uživatelů v kompetence lidských schopností, technologických entit a procesů k efektivnímu vytváření bezpečného digitálního prostředí. Tento koncept je spojen s přesvědčením, že společnosti prokazující schopnost poskytovat a zajišťovat klíčové aspekty bezpečnosti, soukromí, spolehlivosti a etiky dat v rámci svých online programů a zařízení získávají digitální důvěru uživatelů.

Tyto perspektivy sdílejí základní představu, že digitální důvěra zahrnuje očekávání zodpovědného a etického jednání ze strany organizací, jež poskytují digitální technologie a služby. Klade se zde důraz na klíčový prvek, kterým je ochrana osobních údajů a zajištění jejich bezpečnosti. To nezahrnuje pouze digitální aspekty bezpečnosti, ale také dodržování etických standardů.

Narozdíl od důvěry, digitální důvěra nese své specifické charakteristiky a výzvy. Hlavní odlišností vůči důvěře je absence nutnosti osobní komunikace s jednotlivcem – místo toho je důvěra vkládána do systému. Digitální důvěra má za cíl vytvořit pevné pouto mezi uživatelem a danou entitou, jenž uživateli zaručuje bezpečné a spolehlivé uspokojení jeho požadavků. Tato komunikace s digitálními systémy probíhá prostřednictvím internetu a přináší řadu problémů, které je potřeba řešit. Způsob, jakým se tyto výzvy zvládají, může buď posilovat či oslabovat digitální důvěru. [16]

V kontextu těchto výzev a charakteristik hraje bezpečnostní hledisko důležitou roli. V digitálním světě existuje mnoho potencionálních rizik, které mohou ohrozit toto pouto. Závažnou výzvou v této oblasti jsou kybernetičtí útočnici a podvodníci, kteří využívají této digitální důvěry. Kybernetický útočník neboli hacker, může provést útok z jakéhokoli místa na světě a může být obtížné ho vypátrat, což mu dává pocit bezpečí. Porovná-li se riziko odcizení, či zneužití osobních údajů v digitální podobě oproti fyzické podobě, lze předpokládat, že v digitální variantě může být daleko rozsáhlejší a rychlejší, a tím pádem nebezpečnější. Rozsáhlejší z důvodu možnosti postihnutí obrovského množství uživatelů v jediném okamžiku a rychlejší zase proto, že ukrást osobní informace více osob trvá méně času než ve fyzickém světě. Navíc vlastnost okamžitého šíření a zneužití ukradených dat tento proces zrychluje.

Existuje řada různorodých metod, kterými lze provádět útoky, a přitom se nemusí omezovat jenom na útoky proti organizacím spravující tyto data. Tyto útoky mohou směřovat také na jednotlivce, kdy se může jednat o podvodné emaily, vytvoření falešných webový stránek napodobující webové stránky známých firem. Tímto způsobem mohou být jednotlivci oklamáni a dobrovolně poskytnou své osobní údaje. Problém odcizení či zneužití osobních údajů představuje jednu z výzev v digitálním prostředí. Další zásadní rolí je zajištění spolehlivosti digitálních technologií, přičemž musí splňovat očekávání uživatele ve smyslu vykonání funkcí, které od nich uživatel vyžaduje. To zahrnuje dodržování očekávané rychlosti, dostupnosti, ale také konzistentní provoz bez chyb. Jedná se o další aspekt tvořící základ pro hodnocení důvěryhodnosti digitálních technologií. [17]

V současné době se dá identifikovat řada dalších faktorů významně ovlivňujících digitální důvěru, a to jak v pozitivním, tak v negativním světle. Mezi tyto faktory patří psychologické aspekty, které mohou být využity nekalými subjekty v rámci sociálního inženýrství k manipulaci a získání důvěry. Dále se velmi rychle rozvíjí umělá inteligence, což může mít velmi negativní dopad na digitální důvěru. Významnou roli v tomto procesu sehrávají organizace, které tyto digitální technologie a služby tvoří a spravují.

4.1 Digitální důvěru staví organizace

V éře digitálního věku se organizace stávají klíčovými aktéry ve vytváření a udržování důvěryhodného prostředí. Začleňují technologické prvky do co nejvíce aspektů jejich operací a fungování. To klade nároky na uživatele, kteří jsou žádaní důvěřovat jim prostřednictvím nových a hlubších způsobů, od žádosti o jejich osobní údaje po sledování jejich online chování. Zároveň organizace nesou odpovědnost za bezpečnost, spolehlivost, zabezpečení a etický přístup k osobním údajům svých uživatelů.

Nicméně i v této oblasti se mohou objevit technologické problémy. Jedná se například o nevhodné či nelegální sledování uživatelů, zneužití osobních údajů či nedostatečné zabezpečení vůči útokům ze strany hackerů. Tyto problémy mají potenciál vážně poškodit a oslabit digitální důvěru. Jedním z příkladů takového incidentu je případ internetového portálu Yahoo, kdy se hackerům podařilo získat jména, emailové adresy, telefonní čísla, data narození a hesla od jejich uživatelů. Rozsah tohoto útoku byl rozsáhlý, postihl zhruba 3 miliardy uživatelských účtů. [18]

Vzhledem k výše zmíněným problémům je zvýšení digitální důvěry ve své technologie klíčovým úkolem pro organizace. K dosažení tohoto cíle by měly být zohledněny čtyři pilíře digitální důvěry: [19]

- Pilíř 1: Transparentnost a dostupnost
- Pilíř 2: Etika a zodpovědnost
- Pilíř 3: Soukromí a kontrola
- Pilíř 4: Bezpečnost a spolehlivost

4.1.1 Pilíř 1: Transparentnost a dostupnost

První pilíř formuluje koncept, v němž každá organizace by měla praktikovat transparentnost ve všech aspektech interakcí s uživatelem. Uživatelé mohou online shromáždit obrovské množství informací o produktech, službách, jednoduše o tom,

o co mají zájem. Taktéž jsou na internetu schopni najít informace o společnostech, které danou požadovanou subjektivní potřebu nabízí. Lidé projevují sklon poskytnout své osobní data organizacím, ale očekávají, že budou transparentně informování o způsobu uchovávání a využívání těchto dat.

Dostupnost znamená snadný přístup k těmto informacím. Zahrnuje, že by uživatelé měli být schopni rychle a snadno nalézt potřebné informace o produktech, službách, organizaci a dalších náležitých informacích. [19]

4.1.2 Pilíř 2: Etika a zodpovědnost

Technologie mají potencionální temnou stránku. Jejich etický charakter závisí pouze na záměrech tvůrců. Dané technologie nemusí disponovat schopností logického rozlišení toho, jestli se jedná o korektní nebo nekorektní jednání. Tuto schopnost mají hlavně lidé. To znamená, že tvůrce musí vyhodnotit, jakým způsobem se budou technologie využívat a jestli je daný způsob v souladu se základním účelem a principy. [19]

Například firma Volkswagen vytvořila software, který měl oklamat test. V roce 2015 aktivisté odhalili, že automobily této společnosti emitují při běžné jízdě na silnici mnohem více oxidu dusného, než bylo zaznamenáno v testovacích podmínkách. Tato softwarová funkce umožnila vozidlu projít testem, přičemž dokázala rozpoznat, že je testováno a dokázala uměle ovládat vozidlo takovým způsobem, aby obstálo u zkoušky, ale při normální jízdě tato funkce byla vypnuta. [20]

Důležité je poukázat na to, že technologie nemusí rozeznávat, co je správné a špatné, ale vytváří je lidé, kteří o tom již mají schopnost rozhodovat. Potom je na daných tvůrcích, zda se rozhodnou využít sílu této temné stránky.

Při vytváření nových technologií bývá často využívána umělá inteligence pro plnění daných úloh. Využívá se například pro zlepšení služeb zákazníkům, kdy nejčastějším způsobem jsou tzv. chatboti, se kterými zákazníci mohou přímo interagovat. Chatboti umožňují zefektivnit procesy zákaznických služeb a uvolnit čas zaměstnancům, kteří mohou řešit personalizovanější úlohy. Dále se dá umělá inteligence použít při doporučování produktů a nespočetně dalších činnostech. [21]

Dále by měla být povinnost implementovat bezpečnostní opatření s kontrolou, která zabraňuje neetickým nebo nevhodným použitím dané technologie uživatelem. Mělo by to vytvářet zodpovědnost na straně organizace, či poukázat na vlastní zodpovědnost osoby, kdy je osoba jasně varována před negativními následky jeho akcí. Výsledkem

této implementace je možnost zabránění uživatelům interagovat nezodpovědnými nebo nezdravými způsoby. Může se jednat o vytvoření limitů stráveného času, či limitu maximální útraty a podobně. [19]

4.1.3 Pilíř 3: Soukromí a kontrola

Základním prvkem je dodržování předpisů o ochraně údajů, které se zabývají řádným nakládáním s daty. Zaměřují se na to, jak by měly být údaje shromažďovány, ukládány, spravovány a sdíleny s třetími stranami a také na dodržování platných zákonů o ochraně osobních údajů jako je GDPR. [22] [19]

Mnoho společností si zajišťuje důvěru tím, že uživatelé mohou kontrolovat a taktéž nastavovat poskytované informace, které můžou společnosti skladovat a využívat. Jedná se například o osobní údaje typu celého jména, věku, pohlaví nebo také behaviorální data, jako například být údaje o transakcích, podrobnosti o nákupu, předchozí nákupy a dále. [23] [19]

Společnost Google má vytvořenou webovou stránku, na které se uživatelé mohou dovědět mnoho informací o tom, jak se s jejich daty pracuje. Popisuje se zde jaké informace ukládají, z jakého důvodu. Další podstatnou částí je uchovávání informací, kde je popsáno na jak dlouho jsou ukládány, postup smazání, nebo i omezení poskytování některého typu dat, ale bohužel se nedá omezit úplně všechno. [24]

4.1.4 Pilíř 4: Bezpečnost a spolehlivost

Bezpečnost a spolehlivost je dalším základním pilířem pro digitální důvěru. Tato důvěra je poskytnuta organizaci, která je schopna poskytnout pocit bezpečí a spolehlivé funkčnosti vykonávaných úloh požadované uživatelem.

Populárním modelem pro bezpečnost je tzv. triáda CIA, jenž orientuje strategii organizace k celkovému zajištění informační bezpečnosti. Prvky triády patří k nejzákladnějším a nejdůležitějším potřebám k tomu, aby byla zajištěna informační bezpečnost. CIA je tvořeno koncepty důvěrnosti, integrity a dostupnosti. [25]

Důvěrnost je tematicky velmi podobná k pojmu soukromí z již definovaného třetího pilíře. Jedná se o opatření, která jsou navrhnuta takovým způsobem, aby zabránila neoprávněným pokusům o přístup k citlivým informacím.

Integrita definuje přesnost a důvěryhodnost dat po celou dobu jejich životního cyklu. To znamená, že data se nesmí měnit během přenosu a taktéž nesmí být dopuštěno měnění údajů neoprávněnými osobami.

Dostupností se rozumí konzistentní a snadný přístup k daným informacím oběma stranám – uživatelům a společnosti. Zahrnuje to údržbu hardwaru a technické infrastruktury.

Částí tohoto pilíře je spolehlivost, kterou je myšlena pravděpodobnost komponent systému provedení požadované služby bez selhání.

4.2 Přínosy a nevýhody

Digitální důvěra se vztahuje k technologiím, systémům, službám i informacím. Klíčovou roli hraje jak v interakcích jednotlivce, tak ve firemním prostředí. Všechny tyto prvky mají jak svůj pozitivní, tak i negativní potenciál. V rámci této kapitoly představím některé možné přínosy a nevýhody, které se objevují v souvislosti s uspokojením této digitální důvěry v různých oblastech digitálního prostředí.

Cestování a doprava – Využitím cestovních technologií lze efektivněji plánovat cesty, rychle provádět rezervace i navigovat v neznámých lokalitách pomocí GPS aplikací. Díky těmto technologiím je snazší a ekonomicky výhodnější provádět rezervace, zatímco navigace v neznámých lokalitách je pohodlnější díky GPS aplikacím, které mohou fungovat i bez připojení k internetu. Cestovní technologie zároveň přinášejí zvýšení úrovně bezpečnosti. Dokáží poskytovat aktuální informace o provozu na silnicích, místní kriminalitě a nouzových kontaktech. Využití se najde i pro společnosti působící v odvětví poskytování cestovních služeb, které používají tyto technologie ke zlepšení svých produktů a služeb. Jedná se například o letecké společnosti využívající BIG data k předpovídání poptávky cestujících a optimalizaci letových rozvrhů. Také cestovní prostředky, jako jsou letadla, vlaky a lodě, využívají digitální technologie k přesné navigaci po pevnině, ve vzduchu i na moři. [26] [29]

Přístup k informacím – Umožňuje rychlé a komfortní získání informací bez nutnosti složitého vyhledávání, či osobní návštěvy míst. Kvalita není snížena na rozdíl od analogové formy. Informace v analogu se dají snadněji ztratit, zničit, duplikovat. [27]

Automatizace – Systémy mohou pracovat nepřetržitě a zajistit pomoc a služby zákazníkům kdykoliv je potřebují. Každý zákazník obdrží stejně vysokou úroveň služeb s konzistentními informacemi a rychlými reakcemi. Automatizované systémy dokáží shromažďovat a analyzovat data, což podnikům umožňuje získat poznatky o chování zákazníků, jejich preferencích a úrovni spokojenosti. Tyto získané informace se následně využijí ke zlepšení zákaznického servisu a přizpůsobení nabídek podle potřeb zákazníků. Z pohledu organizace to šetří čas a snižuje riziko

lidské chyby. Po automatizaci rutinních úkolů se zvyšuje produktivita, což znamená, že zaměstnanci se mohou soustředit na složitější úkoly. To může zvýšit spokojenost a snížit riziko vyhoření. [28]

Internetové bankovnictví – Využívání internetového bankovnictví přináší několik výhod. Mezi ně patří neustálý přístup k bankovnímu účtu, který je dostupný nepřetržitě. Stačí pouze připojení k internetu a všechny potřebné transakce a úkony lze provést online, což redukuje nutnost fyzické návštěvy banky pro řešení některých záležitostí. Další nespornou výhodou je schopnost snadno převádět peníze mezi účty jak ve stejné bance, tak i mezi jinými bankami. S tím je spojena také funkce online plateb. Možnost sledovat aktivity na finančních účtech může včas odhalit zvláštní odchod peněžních prostředků. Internetové bankovnictví poskytuje i výhody přímo pro banku. Může se jednat o menší riziko lidských chyb, snížení počtu poboček, což má za následek snížení nákladů. Služby elektronického bankovnictví jsou pro zákazníka pohodlnější, což vede ke zvýšení loajality klientů. Základní negativum je tedy možnost, že bezpečnost účtu může být ohrožena hackerskými útoky. Dalším negativem může být nedostatek přímého kontaktu mezi bankou a zákazníkem, kdy člověk může postrádat návštěvu kamenné pobočky v řešení některých záležitostí, a to z důvodu omezování poboček kvůli menšímu zájmu klientů. Stále více lidí raději vše zařídí online, kdy tento trend výrazně zrychlila i pandemie covidu-19. Mnoho klientů si v této době zvyklo řešit většinu záležitostí bez osobního kontaktu. [30] [31] [32]

Bezhotovostní platby – Bezhotovostní platby jsou transakce, které se odehrávají elektronicky bez použití hotovosti. Nejčastěji se jedná o platbu pomocí debetní nebo kreditní karty. Karta je buď vložena do čtečky nebo přiložena k terminálu, a částka se poté automaticky strhne z účtu. Bezhotovostní platby mohou být také vytvořeny jednorázovým příkazem k úhradě nebo pravidelně jako trvalý příkaz. Výhodou těchto plateb je eliminace potřeby manipulovat s hotovostí. Rozvíjí se platby mobilním zařízením jako způsobu bezkontaktního placení. Osoba si může uložit údaje karty do zabezpečené aplikace a při placení může použít svůj mobilní telefon, chytré hodinky nebo jiné zařízení s bezkontaktní technologií. [33]

Elektronické obchodování – Představuje online prostředí, kde se dá nakupovat a prodávat zboží. Jedna z výhod je, že tyto obchody jsou k dispozici neustále. Zákazníci mají možnost nakupovat kdykoli, stačí navštívit webové stránky prodejce. Tato možnost výrazně zvyšuje pohodlí, protože produkty lze objednat odkudkoli na světě. Dalším relevantním faktorem může být úspora času, protože nákup přes internet

trvá méně času než návštěva kamenného obchodu a hledání konkrétního produktu. Taktéž srovnání cen v různých obchodech pro stejný produkt je daleko snadnější. Online prostředí elektronického obchodování, známého také jako e-commerce, poskytuje rozsáhlý sortiment zboží a služeb, což umožňuje zákazníkům provádět rozmanitý výběr produktů a služeb a vybrat si ty nejvhodnější, na rozdíl od tradičních fyzických návštěv, kde je dostupný pouze omezený sortiment. Toto souvisí s dostupností, protože zákazníci mohou rychle procházet kategorie zboží a najít požadovaný produkt. Naopak mezi nevýhody může patřit nemožnost osobního vyzkoušení zboží, možnost zpoždění nebo poškození během doručení. [34] [35]

Zabezpečenost dat – V souvislosti používání digitálních technologií, služeb atd. je shromažďováno a ukládáno velké množství informací. Tyto informace se mohou týkat jak jednotlivců, tak organizací. Jediné narušení bezpečnosti může mít za následek, že velké množství soukromých informací se dostane do rukou zločinců, obchodních rivalů nebo jiných škodlivých entit. [36]

Problematika ochrany soukromí – Existuje cílená reklama, kdy digitální zařízení ví přesně co jsme koupili, kde jsme byli, nebo jaké služby či produkt si člověk chce zakoupit. I toto má dvě strany. Na jednu stranu to může být užitečné, protože například Netflix může na základě tohoto sledování doporučit seriál, film a tím pádem to dokáže ušetřit čas. Avšak na druhou stranu to může mít velké nevýhody, protože tyto informace mohou být použity pro škodlivé účely, pokud padnou do nesprávných rukou. Mohou být poskytnuty komukoli, kdo je ochotný za ně zaplatit. V téhle digitální éře již nejde mít absolutní kontrolu nad tím, jak jsou šířeny. Dá se říct, že se v této době staly prodejním zbožím. [37]

Manipulace digitálních médií a dezinformace – Velké množství dostupných zdrojů na internetu komplikuje hodnocení důvěryhodnosti některých z nich. V dnešní době již informace nepřichází pouze prostřednictvím novin, ale lze k nim přistupovat i pomocí internetových zdrojů, sociálních sítí jako je Facebook a dalších dostupných prostředků. Tímto způsobem se digitální média, jako jsou fotografie, zvuk a videa, staly jednoduše upravitelnými. Už nemusí být snadné rozlišit mezi tím, co je skutečné a co není. Fotografie lze upravovat pomocí například Photoshopu, ale i ostatní média jdou jednoduše upravovat pomocí k tomu příslušných nástrojů. Dnes může kdokoliv digitálně vytvářet, šířit anebo získávat obrázky, videa, texty. Algoritmy nerozlišují mezi potencionálními pravdivými a nepravdivými informacemi a tím pádem je možné

se dostat k potenciálně falešným médiím kdykoliv a kdekoliv. V důsledku toho může dezinformace na internetu dosáhnout daleko většího dosahu.[38]

Je zřejmé, že digitální důvěra s sebou nese pozitivní aspekty, jak je poukázáno například v oblasti usnadnění cestování, využívání internetového bankovnictví, e-commerce a v mnoha dalších oblastech, které nejsou specifikovány v této práci. Nicméně s tím souvisí i nepříznivé faktory, neboť mohou vyvolat závažné problémy. Především se jedná o problematiku týkající se zabezpečení dat, ochrany soukromí a manipulace digitálních médií a dezinformace.

4.3 Faktory ohrožující digitální důvěru

Existuje mnoho způsobů, jak ohrožovat digitální důvěru v digitálním světě. Jedním z hlavních problémů jsou hackeři. Cílem hackera může být ukradnutí informací, paralyzování systémů a často to souvisí k vymáhání výkupného. [39] Útočníci například vytvářejí podvodné emaily, které následně rozesílají lidem. Mohou využívat záminku toho, že se jedná o varování ohledně chyby v bezpečnosti systému nebo jinou důležitou informaci s cílem přesvědčit uživatele o pravosti zprávy. Tento druh podvodů spadá do oblasti phishingu. Pokud je celkově podvod proveden dobře a uživatel nemá povědomí o rizicích phishingu nebo zkušenost s ním, mohou být jeho data poslána útočníkovi. Povedený útok vypadá tak, že uživatel klikne na odkaz v emailu a následně je přesměrován na falešnou webovou stránku, jež se vizuálně snaží napodobit originální stránku. Zde je požádán o to, aby vyplnil své přihlašovací údaje, často včetně citlivých informací, jako je číslo platební karty a její ověřovací třímístné číslo. Jakmile jsou tato data vyplněna a odeslána, dostávají se do rukou útočníka, který z účtu odčerpá možné finanční prostředky. [40]

Digitální důvěra má své výhody, ale je také velmi zranitelná. Jedná se o cenný základ pro fungování společnosti v digitálním prostředí, ale může čelit hrozbám z různých perspektiv. To zahrnuje nejen potencionální rizika z hlediska organizací uchovávající citlivá uživatelská data, ale i individuálních osob, které jsou taktéž náchylné k útokům a manipulaci.

4.4 Shrnutí

Existence systému představuje hlavní rozdíl mezi důvěrou a digitální důvěrou. Přístup k těmto systémům se uskutečňuje přes internet, což přináší řadu výzev. Jednou z hlavních výzev je zajištění bezpečnosti, kdy systém čelí hrozbám ze strany hackerů. Hackeři mohou provést své útoky prakticky z jakéhokoliv místa na světě a jejich

vypátrání může být velmi obtížné. Dále to jsou podvodníci, zaměřující se hlavně na jednotlivce. Jedná se například o podvodné emaily a falešné webové stránky. Další výzvou je zajištění spolehlivosti digitálních technologií, kdy uživatelé očekávají vykonávání funkcí, které jsou od nich vyžadovány.

Systémy, digitální technologie a služby jsou vytvářeny organizacemi. K budování digitální důvěry existují 4. pilíře. První pilíř pojednává o potřebě transparentně informovat o způsobu uchovávání a využívání dat uživatele. Druhý pilíř poukazuje na to, že technologie nemusí disponovat schopností rozpoznání korektního a nekorektního jednání. To znamená, že etický charakter závisí na záměrech tvůrců. Další částí je zodpovědnost, kdy by se měla organizace snažit zabránit nevhodnému použití digitálních technologií. Třetí pilíř se zaměřuje na dodržování předpisů o ochraně údajů. Čtvrtý pilíř pojednává o vytvoření pocitu bezpečí pro uživatele a zajištění spolehlivého plnění funkcí, jež jsou od těchto technologií požadovány.

Díky uspokojené digitální důvěře mohou organizace získat nové uživatele, zákazníky, a naopak uživatelé mohou díky tomu využívat výhody, jako je například internetové bankovnictví a nakupování prostřednictvím internetových obchodů.

5. Bezpečnost a zvyšování digitální důvěry

Tato kapitola se bude věnovat prvkům, které přispívají k posílení digitální důvěry. Konkrétně se zaměří na koncepty elektronických podpisů, pečetí a razítek, což jsou klíčové nástroje pro zabezpečení a zdůvěryhodnění digitálních dokumentů. Dalším konceptem je vícefaktorová autentizace, která zvyšuje bezpečnost digitálních účtů před neoprávněným přístupem a potencionálním zneužitím.

5.1 Elektronický podpis, pečeť a razítko

Dokument v analogové podobě může, někdy i musí být vlastnoručně podepsán. Spolu s digitálním světem se rozvíjí i způsob podepisování dokumentů. Vznikají mechanismy, které mají poskytnout danou jistotu, že obsah dokumentu nebyl změněn a že pochází ze správného zdroje. Elektronický podpis označuje data, která jsou připojena nebo logicky spojena s jinými daty a jsou použita uživatelem k podepsání dokumentů v digitální podobě. [41]

Existují 3 typy a úrovně elektronického podpisu používajícího se v jiných situacích. Rozdělují se od nejvyšší úrovně po nejmenší.

5.1.1 Kvalifikovaný elektronický podpis

Jedná se o nejvyšší a nejkvalitnější úroveň, kdy je podpis vytvořen prostřednictvím kvalifikovaných certifikátů, vydané certifikační autoritou. V Česku existují tři veřejné certifikační autority, u kterých si každý může zajistit svůj kvalifikovaný podpisový certifikát – PostSignum, eIdentity, První certifikační autorita. Existuje čtvrtá certifikační autorita, ale je určena výhradně pro vybrané subjekty veřejné správy. Může být i kvalifikovaná certifikační autorita z EU. Další podstatnou části kvalifikovaného elektronického podpisu je, že musí být nadále vytvořen pomocí kvalifikovaných prostředků pro vytváření elektronických podpisů, což jsou v praxi nejčastěji čipové karty a USB tokeny, které prošly potřebnou certifikací. [42] [43]

5.1.2 Zaručený elektronický podpis založený na kvalifikovaném certifikátu

Představuje specifický typ elektronického podpisu, který se odlišuje od kvalifikovaného elektronického podpisu v absenci požadavku na použití kvalifikovaného prostředku, jako je již zmíněná čipová karta nebo USB token. Podmínkou zůstává stále to, že tento podpis musí být založen na kvalifikovaném certifikátu. To je výhodné pro posílání dokumentů elektronickou formou státní správě. Tyto úřady mají zákonnou povinnost dokument s tímto typem podpisu akceptovat. [42] [43]

5.1.3 Zaručený elektronický podpis

Jedná se o nejnižší úroveň – nejméně kvalitní. Pro své vytvoření nepotřebují kvalifikovaný certifikát. Stačí jakýkoli certifikát pro elektronické podepisování, i například testovací, který si může vyrobit kdokoli. Tento typ elektronického podpisu je možné používat tam, kde se nejedná o elektronickou komunikaci se státní správou. [42] [43]

5.2 Elektronická pečeť a razítko

Alternativou pro elektronický podpis pro právnické osoby je elektronická pečeť. Elektronický podpis patří fyzické osobě a je brán jako jednoznačný projev vůle konkrétní osoby, zatímco elektronická pečeť existuje s cílem zaručit pravost a neměnnost dokumentu. Jedná se o důkaz toho, že dokument vydala určitá právnická osoba. Elektronická pečeť se používá v případech, kdy právní předpis nestanoví jako náležitost právního jednání elektronický podpis. Jedná se především o hromadné a automatizované operace s dokumenty. [44] [45]

Součástí elektronického podpisu nebo elektronické pečetě může také být časové razítko. To zaručuje, že uvedená data v elektronické podobě existovala v určitý časový okamžik v dané podobě. Časová razítka poskytují různé certifikační autority, což znamená že přesný čas se nezjišťuje u odesílatele, ale u certifikační autority, takže čas nemůže být zfalšován tvůrcem dokumentu. Další výhodou je prodloužení platnosti elektronického dokumentu. Elektronický podpis má platnost 1 rok. Pokud je opatřen časových razítkem, prodlouží se jeho platnost až na 5 let. [46] [47]

5.3 Vícefaktorová autentizace

Autentizací se rozumí proces, kde subjekt dokazuje vlastnictví anebo kontrolu nad konkrétní identitou. To je prováděno tím, že subjekt poskytuje tajné informace, známé pouze subjektu a autentizačnímu systému. Zmiňované tajné informace mohou být ve formě uživatelského jména, PINu, hesel, řešení hádanky a dalších mnoha způsobů. Dokázání vlastnictví dané identity je provedeno subjektem tím způsobem, že subjekt poskytuje identitu a jeden nebo více autentizačních faktorů. Autentizační faktor představuje prvek, který subjekt předkládá a zná pouze on sám, nebo který může předložit, čímž prokazuje své jednoznačné vlastnictví identity. [48]

Obecně se používají tři základní typy autentizačních faktorů:

- Něco, co subjekt zná:
  - Heslo, PIN, hádanka atd.
- Něco, co subjekt má:
  - Telefonní číslo, USB token atd.
- Něco, čím subjekt je:
  - Biometrie, otisk prstu atd.

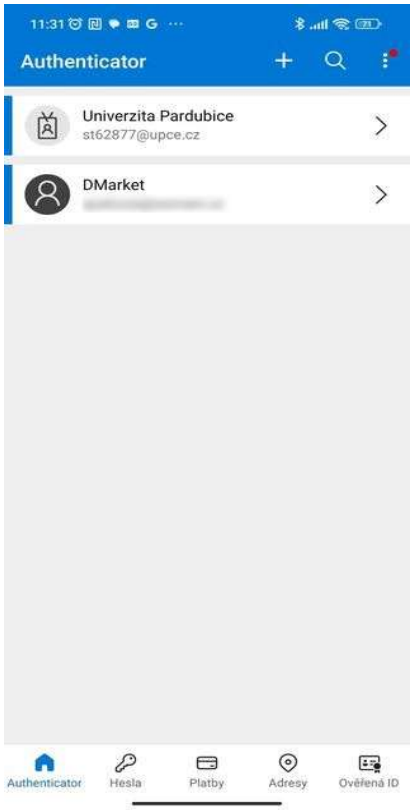
Z hlediska autentizace je důležitý počet faktorů, které jsou vyžadovány pro úspěšnou autentizaci. Jedná se o:

- Jednofaktorovou autentizaci – Je vyžadován jediný důkaz autentizace, například znalost hesla, či PINu. Jednofaktorová autentizace je rychlá a pohodlná, ale také nejvíce zranitelná vůči útokům. [49]
- Dvoufaktorová autentizace – Jsou požadovány dva různé autentizační faktory. Za cíl se klade zvýšení zabezpečení citlivých informací. Proces dvoufaktorové autentizace vyžaduje, aby dvě dané ověřitelné informace patřily do různých kategorií. Například při přihlašování mohou uživatelé poskytnout svá uživatelská jména a hesla (něco, co subjekt zná) a současně prokázat to, že mají

ve svém držení fyzický přístupový klíč (něco, co subjekt má), což může být například jejich smartphone. [49]

- Vícefaktorová autentizace – V případě vícefaktorové autentizace jsou uživatelé nuceni předložit více než jednu ověřitelnou informaci pro úspěšné ověření. Dvoufaktorová autentizace je považována za jednu z forem vícefaktorové autentizace, neboť vyžaduje poskytnutí více než jedné autentizační informace, ale obvykle se jedná o více než dva autentizační prvky. Při procesu přihlašování je uživatel požádán o poskytnutí něčeho, co zná, něčeho, co má a něčeho, čím je. [49]

Příkladem může být Microsoft Authenticator, jako dvoufaktorové ověřování sloužící pro potvrzení přihlášení. Zastupuje to, že subjekt něco má.



Obrázek 4: Microsoft Authenticator

Zdroj: Vlastní zpracování z (aplikace Microsoft Authenticator)

5.4 Shrnutí

Kapitola bezpečnost a zvyšování digitální důvěry se zaměřuje na zabezpečení digitálních dokumentů a účtů. Jedním z prvků k tomu sloužící je elektronický podpis, jenž je ekvivalentem ručního podpisu. Existuje více úrovní a podle toho se mění jeho možnost využívání. Nejvyšší úrovní je kvalifikovaný elektronický podpis, který má

být vytvořen pomocí kvalifikovaného prostředku a je potřeba zajistit kvalifikovaný certifikát u certifikační autority. Nižší úroveň je zaručený elektronický podpis založený na kvalifikovaném certifikátu, kde rozdílem je, vůči výše zmíněnému podpisu, absence kvalifikovaného prostředku. Nejnižší úrovní je zaručený elektronický podpis, který nepotřebuje ani kvalifikovaný certifikát. Právnické osoby využívají elektronickou pečeť. Existuje časové razítko, které prodlužuje platnost elektronických dokumentů a potvrzuje jejich existenci v určitém časovém období.

Další řešený prvek je vícefaktorová autentizace, která vyžaduje od uživatele poskytnutí něčeho, co zná, něčeho, co má a něčeho, čím je. Dvoufaktorová autentizace je jedna z forem, která spadá do tohoto rámce.

Tyto prvky mají za úkol zvýšit digitální důvěru v oblastech digitálních dokumentů a účtů. V oblasti digitálních dokumentů je úkolem potvrzení identity podepisující osoby a ujištění o tom, že obsah dokumentu nebyl po podepsání změněn. V oblasti účtů se jedná o zvýšení ochrany před neoprávněným přístupem.

6. Umělá inteligence

Umělá inteligence začíná být důležitým faktorem v rozvoji lidstva, a to díky svému stále se rozšiřujícímu využití v různých oblastech každodenního života. Nachází svou roli v nakupování online a reklamě, digitálních osobních asistentech, v autonomních vozidlech a v mnoha dalších aspektech. [50]

Umělá inteligence je velmi široký obor, kdy se nejedná o jednotlivý počítačový program nebo aplikaci. [51] Jedná se o počítačový systém, který bude napodobovat kognitivní funkce spojené s lidskou inteligencí, jako je schopnost rozumět a reagovat na mluvený nebo psaný jazyk, analyzovat data a mnoho dalšího. Často je AI považována jako samostatný systém, ale jedná se o soubor technologií implementovaných do systému pro umožnění schopnosti uvažovat, učit se a jednat za účelem řešení komplexních problémů. [52]

K umělé inteligenci se již od 50 let 20 století vztahuje Turingův test. Jedná se o test, který postaví lidské respondenty proti stroji, aby otestoval schopnost stroje vykazovat lidské reakce a inteligenci. [53] Ale skutečným záměrem není, aby stroj napodoboval lidské chování, protože to zahrnuje nejen inteligenci, ale také prvky jako jsou náladovost a hloupost. Cílem umělé inteligence má být splnění zadání zadavatele a činit rozhodnutí rychleji a lépe než člověk, nikoliv člověka imitovat. [51]

6.1 Metody umělé inteligence

Strojové učení

Strojové učení je podmnožinou umělé inteligence. Umožňuje stroji automatizovaně získávat dovednosti a zlepšovat své schopnosti na základě praktických zkušeností. Vstupní data spolu s výstupem jsou stroji předána během fáze učení. Strojové učení využívá algoritmy pro analýzu rozsáhlých datových souborů, učení se z jejich poznatků a následné přijímání informovaných rozhodnutí. [52] [54]

Hluboké učení

Jedná se o podmnožinu strojového učení, která umožňuje AI učit a zlepšovat se na základě zpracování dat. Hluboké učení pracuje s umělými neuronovými sítěmi, navrženými tak, aby napodobovaly způsob, jakým lidé myslí a učí se. Neuronové sítě jsou vrstvy uzlů a uzly jsou propojeny s okolními vrstvami na základě přiřazených vah. Větší váha u uzlu znamená, že bude mít silnější vliv na následující vrstvu uzlů. Hluboké učení má v sobě 3 hlavní vrstvy. Jedná se o vstupní, skrytou a výstupní vrstvu. Ve skryté vrstvě jsou vypočtené hodnoty, které nejsou pozorovatelné v tréninkové sadě. Čím více skrytých vrstev existuje, tím je síť hlubší. [55] Pro tuto metodu je potřeba obrovské množství dat pro získání přesných výsledků. [56] [51]

Zpracování přirozeného jazyka

Představuje schopnost počítačů rozpoznávat a interpretovat lidský jazyk v jeho mluvené i psané formě. Využívá se zde umělá inteligence pro zpracování přirozeného jazyka a přijímání vstupu z reálného světa, jeho zpracování a porozumění s cílem toho, aby ho počítač chápal. Jedná se o klíčovou součást systémů řízených umělou inteligencí, které interagují s lidmi, a to jak prostřednictvím textových, tak hlasových vstupů. [57] [51]

Kognitivní techniky

Jedná se o stroje, jejichž úkolem je učit se, uvažovat a navazovat přirozenou komunikaci s lidmi. Tyto systémy jsou schopny zpracovat nestrukturovaná data, jako jsou obrázky, texty a řeč a vyvodit z toho závěry. Taktéž dokáží uvažovat, rozhodovat a zlepšovat své schopnosti na základě zkušeností. Navíc jsou schopny interagovat s lidmi v přirozeném jazyce, porozumět různým situacím a poskytovat personalizované odpovědi. [58] [51]

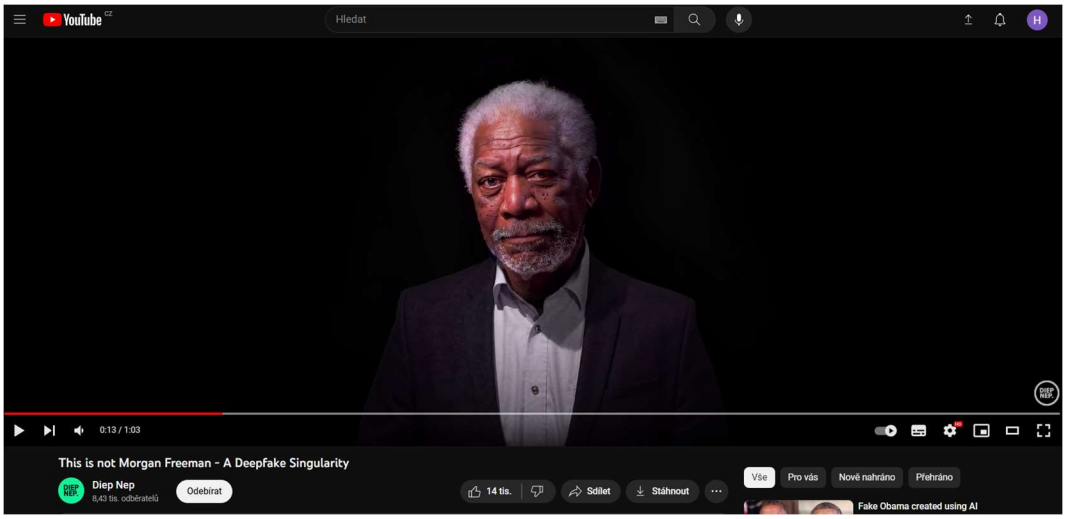
Počítačové vidění

Počítačové vidění je oblast, jenž pojednává o porozumění a interpretaci obsahu z vizuálního výstupu, jako jsou obrázky, či videa. Systémy v oblasti počítačového vidění mají schopnost vidět, identifikovat a pochopit vizuální svět tím, že analyzují vzory a využívají hlubokého učení, což je proces simulující lidské vidění. Pro účely výcviku hlubokého učícího algoritmu, který by se mohl naučit specifické charakteristiky a díky tomu rozpoznat určitý objekt, je zapotřebí velké množství dat. [59] [50]

6.2 Deepfake a dezinformace

Umělá inteligence má v mnoha oblastech určité výhody, ale taktéž může velmi jednoduše narušit digitální důvěru, neboť se jejím použitím dá velmi snadno ovlivnit chování lidí. Jedním ze způsobů může být změna jejich informačního prostředí, což může mít za následek změnu přesvědčení a rozhodování v závislosti na nových informacích nebo zkušenostech. [60]

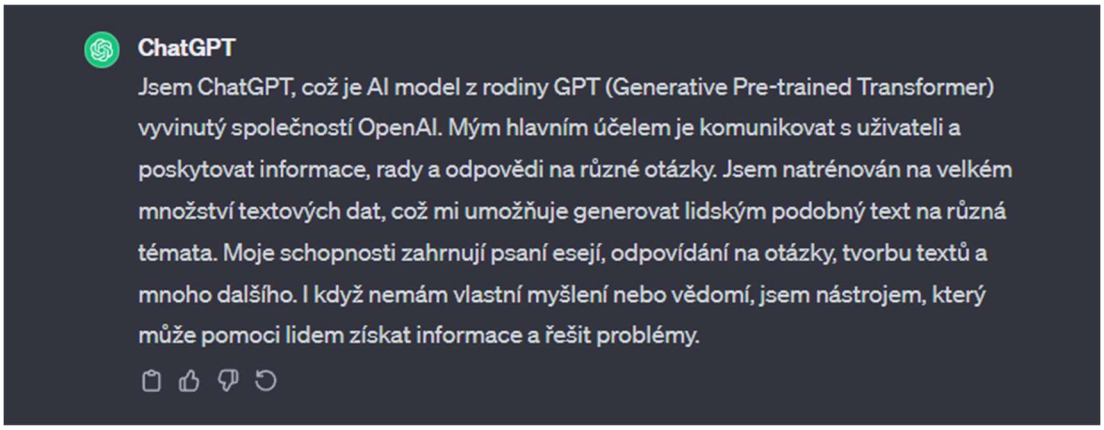
Kombinace umělé inteligence, počítačové grafiky a syntézy řeči dává možnost vytvářet deepfakes. Jedná se o realistický multimediální obsah, kde téměř každý jednotlivec může zdánlivě provádět nebo říkat cokoli, a to v podobě videa nebo audia s vysokou realističností. Možnost vytvořit deepfake dané osoby závisí na množství audiovizuálních dat, která jsou o ní k dispozici. *„Tento typ obsahu dokáže přivodit nezvratné přesvědčení o věcech, které se nikdy nestaly“.* [60] Díky těmto nástrojům mají lidé možnost vytvářet realistická videa s fiktivním obsahem, jež mohou být zneužita pro manipulaci, šíření dezinformací nebo poškození reputace politiků, či známých osobností. Na internetu lze nalézt videa vytvořena pomocí umělé inteligence, v nichž vystupují významné osobnosti přednášející texty nebo provádějící činnosti, které nikdy ve skutečnosti nevykonaly.



Obrázek 5: Deepfake

Zdroj: https://www.youtube.com/watch?v=oxXpB9pSETo

Mimo videa a obrázky může být umělá inteligence využita k šíření dezinformací i v textové podobě. Texty jsou vytvářeny chatboty, například ChatGPT. Jak sám sebe popisuje tento chatbot je uvedeno na Obrázku 6.



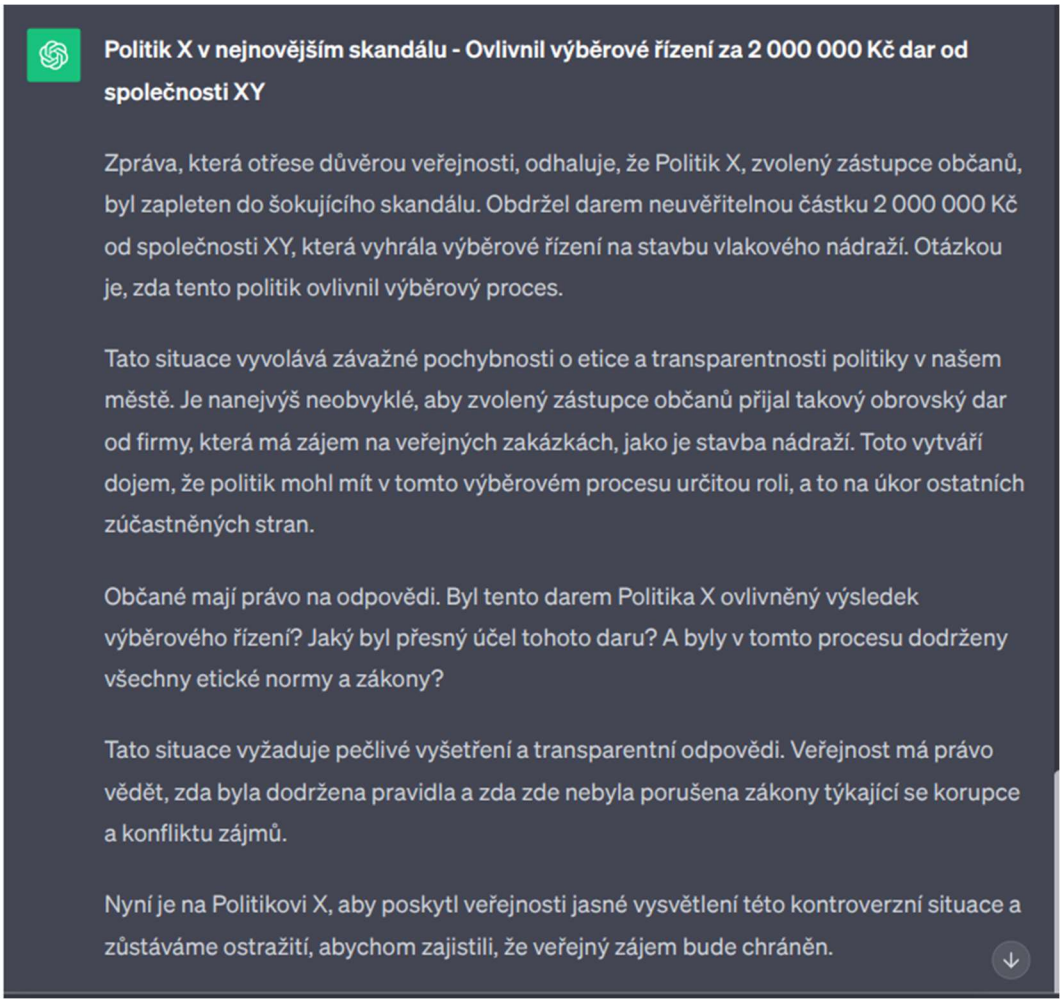
Obrázek 6: Popis ChatGPT

Zdroj: ChatGPT

Jak sám uvedl, mezi jeho schopnosti patří i tvorba textů, tím pádem dokáže vytvořit velmi propracovaný text na různá témata s napojením na dezinformaci. Nechal jsem jej vytvořit text s tímto vstupem:

„Politik X obdržel dar ve výši 2 000 000 Kč od společnosti XY za jejich úspěšné vyhrané výběrové řízení na stavbu vlakového nádraží. Vytvoř to jako mediální skandál, že politik výběrové řízení nějak ovlivnil, co nejvíce autenticky, aby tomu lidé věřili. Nebude tam žádná mediální společnost, jméno autora příspěvku.“

Odpověď ChatGPT je uvedena na obrázku 7.



Obrázek 7: ChatGPT – vytvoření textu

Zdroj: ChatGPT

Podle mého názoru dokázal během několika vteřin vytvořit velmi věrohodný text na zadané téma. Poté může člověk s chatbotem nadále pracovat a vytvořit ještě kvalitnější text. Publikace takové zprávy, jejíž celý obsah je založen na fikci, by mohla cílené osobě způsobit vážné nepříjemnosti.

V éře umělé inteligence se stává tvoření deepfake videí, obrázků a šíření dezinformací snadnější a nebezpečnější. S neustálým vývojem umělé inteligence bude v budoucnu těžké věřit jakýmkoliv informacím.

7. Dotazník

Předchozí kapitoly, které popisovaly charakteristiky aspektů tématu digitální důvěry, se staly zdrojem pro navržení otázek pro dotazníkový průzkum.

Základní postup pro zpracování, navržený v **kapitole 1.1.,** byl nyní detailněji rozpracován.

Detailní postup:

1. **Výběr respondentů** – Zaměření dotazníku je výhradně na mladší generaci, konkrétně na studenty z fakult UPCE. Tento zaměřený výběr umožní případný další výzkum srovnání postojů a zkušeností mé cílové skupiny se starší generací. Pokud by se někdo rozhodl rozvíjet téma v rámci starší populace, mohlo by dojít k zajímavým kontrastům mezi oběma skupinami.
2. **Cílový počet 100 studentů** – Záměrně byl určen cílový počet 100 respondentů s úmyslem získat soubor odpovědi z různých fakult, kde každá má svůj unikátní charakter a přístup, což může ovlivnit jejich postoje k probíraným tématům.
3. **Revize odpovědí** – Zahrnuje ověření všech získaných odpovědí a případnou reakci.
4. **Analýza frekvence odpovědí a test nezávislosti** – Provedení analýzy frekvence výskytu odpovědí na jednotlivé otázky a následně dva testy nezávislosti. Cílem prvního testu bude zkoumání možné závislosti mezi odpověďmi na otázky 2 a 3. Druhý test se bude soustředit na zkoumání možných vztahů mezi pohlavím respondentů a odpověďmi na otázku 10.
5. **Celkové vyhodnocení** – Celkové vyhodnocení výsledků průzkumu.
6. **Zhodnocení výzkumu** – Zhodnocení provedeného výzkumu, případná doporučení a možnosti dalšího rozvoje výzkumu.

Průběh:

Dotazníkové šetření probíhalo prostřednictvím online dotazníku vytvořeném pomocí Google formuláře. Ke sdílení odkazu a jeho následné rozesílání studentům UPCE byly z velké části použity sociální sítě. První fáze šíření dotazníku sestávala z čistě z mých skupin a kamarádů. V této fázi na dotazník odpovědělo přibližně 70 respondentů. Jednalo se ovšem o neuspokojivý výsledek, na jehož základě byla vymyšlena a zahájena druhá fáze, spočívající v osobním oslovování studentů na fakultách Univerzity Pardubice s žádostí o vyplnění dotazníku. Studentům, kteří projevili zájem, byl nasdílen odkaz prostřednictvím sociálních sítí či emailu. Tento přístup vedl k získání celkově 121 vyplněných dotazníků. Dotazník byl pro sběr odpovědí celkově aktivní po dobu přibližně dvou týdnů.

7.1 Prvky digitální důvěry

Prvky zdůrazněny v této kapitole, vzešlé z charakteristik aspektů digitální důvěry, budou zakomponovány do otázek v dotazníku.

Jedná se o tyto prvky:

Digitální identifikační doklady: Zkoumání povědomí studentů o mobilní aplikaci eDoklady a její možné budoucí používání. Dále zjištění názoru na bezpečnost z hlediska fyzického či digitálního dokladu.

Únik soukromých dat: Postoj k možnému zneužití osobních informacích a případná reakce vůči organizaci.

Digitální nástroje: Týká se míry používání bezhotovostních plateb, pohledu na bezpečnost a využívání elektronického podpisu.

Ochrana účtu: Zkoumání názoru na zabezpečení digitálních účtů pomocí vícefaktorové autentizace.

Online řešení záležitosti: Týká se preference řešení záležitosti.

Zisk informací: Zahrnuje preferenci způsobu, jakým studenti získávají informace a pohled na získané informace v digitální formě z hlediska falešnosti.

Umělá inteligence: Zkoumání postojů a vnímání implementace umělé inteligence v různých oblastech, zahrnující i negativní aspekty jejího využití.

7.2 Výzkumný problém

Cílem tohoto výzkumu je provést analýzu digitální důvěry s ohledem na její komplexní charakter, zasahující do mnoha oborů a následně zkoumat, jak tato specifická forma důvěry ovlivňuje postoje jednotlivců k otázkám v oblasti digitální bezpečnosti, ochrany osobních údajů a jejich názorů na umělou inteligenci, v souladu s uvedenými prvky digitální důvěry. Tato témata byla nastíněna v předešlé části práce.

7.3 Analýza dotazníku

Dotazník vyplnilo celkem 121 respondentů. Z důvodu neúplného vyplnění dotazníku jedním respondentem bylo nutno anulovat jeho odpovědi, což vedlo ke snížení celkového počtu na 120.

7.4 Analýza jednotlivých odpovědí

Na začátku dotazníku byly žádány základní osobní údaje, jako je studijní program a pohlaví, pro identifikaci respondentů

Váš studijní program a pohlaví:

Studijní program byl prezentován ve třech možnostech odpovědí: bakalářský, magisterský nebo inženýrský a doktorský. Nejvíce respondentů momentálně studuje na bakalářské úrovni, následované menšinou na úrovni magisterského/inženýrského studia, zatímco žádný respondent nebyl zaznamenán pro doktorský program.

Co se týče pohlaví, respondentů mužského a ženského pohlaví bylo téměř stejné množství, a jejich podrobné rozdělení je uvedeno v následující tabulce.

Váš studijní program		Pohlaví	
Bakalářský	99 (83 %)	Muž	69 (57,5 %)
Magisterský/inženýrský	21 (18 %)	Žena	50 (41,67 %)
Doktorský	0	Jiné	1 (0,83 %)

Tabulka 1: Studijní program a pohlaví

Zdroj: Vlastní zpracování

Tabulka 2 reprezentuje procentuální zastoupení fakult.

Fakulta	Procentuální zastoupení
Dopravní fakulta Jana Pernera	22 %
Fakulta ekonomicko-správní	28 %
Fakulta elektrotechniky a informatiky	16 %
Fakulta filozofická	15 %
Fakulta chemicko-technologická	19 %

Tabulka 2: Procentuální zastoupení fakult

Zdroj: Vlastní zpracování

Po identifikaci respondenta následují již vybrané otázky na téma digitální důvěry.

Otázka 1: Jak byste charakterizovali termín "digitální důvěra" a co pro vás přesně znamená?

Odpovědi na tuto otázku byly velmi různorodé. Studenti zde popisovali jejich vnímání termínu digitální důvěra, přičemž se odpovědi často tematicky opakovaly. Nejčastěji se vyskytující témata byla rozdělena do několika hlavních kategorií.

První kategorie: Bezpečnost osobních údajů – V této kategorii se studenti souhrnně vyjádřili tím způsobem, že digitální důvěra pro ně znamená chránění a zamezení šíření jejich osobních informací na internetu. Vkládají svou důvěru v zacházení s osobními daty a zabezpečení systému, digitální instituci nebo online obchodu, kterým svá osobní data svěřují. Tato řešená kategorie je často spojována s důvěrou v digitální

technologie, systémy, aplikace a digitální zařízení. Dle mého názoru je nejvíce charakteristická odpověď shrnující i všechny ostatní odpovědi v této kategorii:

„Nebát se o svá citlivá data v online prostředí. Mít jistotu, že mé osobní údaje nebudou šířeny dále a budou sloužit potřebám pouze dané aplikaci, platformě.“

Druhá kategorie: Získávání informací na internetu – Obsah této kategorie souhrnně pojednává o důvěře v informace získaných na internetu. Respondenti ji berou jako míru důvěry ve zprávy, informace atd. Za shrnující odpověď na mou otázku bych označil tuto:

„Zda důvěřuji informacím na internetu“

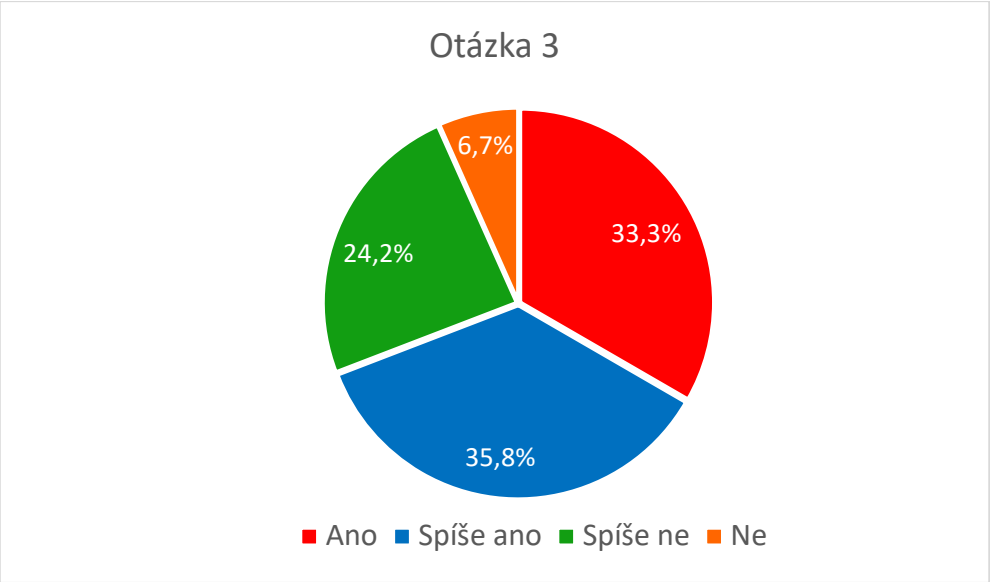
Třetí kategorie: Důvěra v lidi a organizace – V této kategorii rozumí studenti termínu digitální důvěra jako souvislosti s interakcemi s lidmi a organizacemi na internetu. Chápou ji jako míru víry v osoby či organizace vystupující online, nebo jako důvěru budovanou prostřednictvím digitální komunikace – emaily, zprávy na sociálních sítích. V této kategorii bych vyzdvihl tuto odpověď: *„Představím si pod tím důvěru, která je budovaná prostřednictvím digitálních komunikačních kanálů“.*

Otázka 2: Slyšeli jste o mobilní aplikaci eDoklady (jedná se o aplikaci, ve které bude možné mít své identifikační doklady v digitální formě)?

Tato otázka se týká povědomí o mobilní aplikaci eDoklady, která bude nabízet uchování svých identifikačních dokladů v digitální podobě. Byly zde na výběr pouze dvě odpovědi, a to „Ano“ a „Ne“. Získané výsledky ukazují, že 51 % respondentů má o této aplikaci povědomí, zatímco 49 % nemá. Otázka měla za úkol zjistit informovanost o problematice digitalizace identifikačních dokladů a funguje jako vstupní bod pro následné zkoumání, rozvinuté v následujících otázkách. Zastupuje prvek „digitální identifikační doklady“ vyskytující se i v otázkách 3 a 4.

Otázka 3: Uvažujete o tom, využívat možnost prokazování se touto aplikací, až to bude možné?

Otázka navazuje na předešlou otázku o povědomí aplikace eDoklady a zaměřuje se na postoj respondentů k jejímu budoucímu využívání. Respondenti měli na výběr ze čtyř možných odpovědí – „Ano,“ „Spíše ano,“ „Spíše ne“ a „Ne.“ Pozitivním směrem se k využívání aplikace vyjádřilo 69,1 % studentů. Pouze 6,7 % respondentů uvedlo, že nemá v úmyslu tuto aplikaci využívat. Tyto výsledky vyznačují náklonnost studentů k používání digitálních identifikačních dokladů.

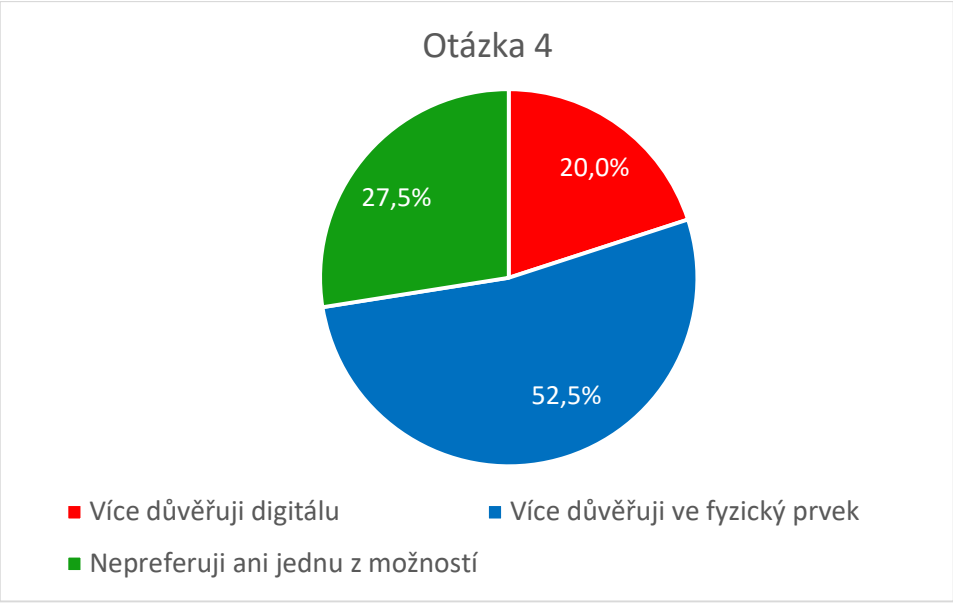


Graf 1: Otázka 3 – Uvažování o používání aplikace

Zdroj: Vlastní zpracování

Otázka 4: Domníváte se, že je pro Vás bezpečnější mít identifikační doklad (například občanský průkaz) v podobě karty, nebo v digitální podobě v aplikaci. Jaký je váš názor na bezpečnost těchto informací?

Poslední otázka týkající se identifikačních dokladů se zabývá názorem studentů na bezpečnost v různých formách – digitální a fyzické. Dotazník umožnil vybírat ze tří možností – „Více důvěřuji digitálu," „Více důvěřuji ve fyzický prvek," „Nepreferuji ani jednu z možností." Vzhledem k získaným odpovědím vykazuje průzkum, že pro studenty je fyzická podoba bezpečnější než digitální. Možnost „Více důvěřuji ve fyzický prvek" zvolilo 52,5 % respondentů, 27,5 % nepreferovalo ani jednu možnost a pouze 20 % projevilo větší důvěru v digitální formu.

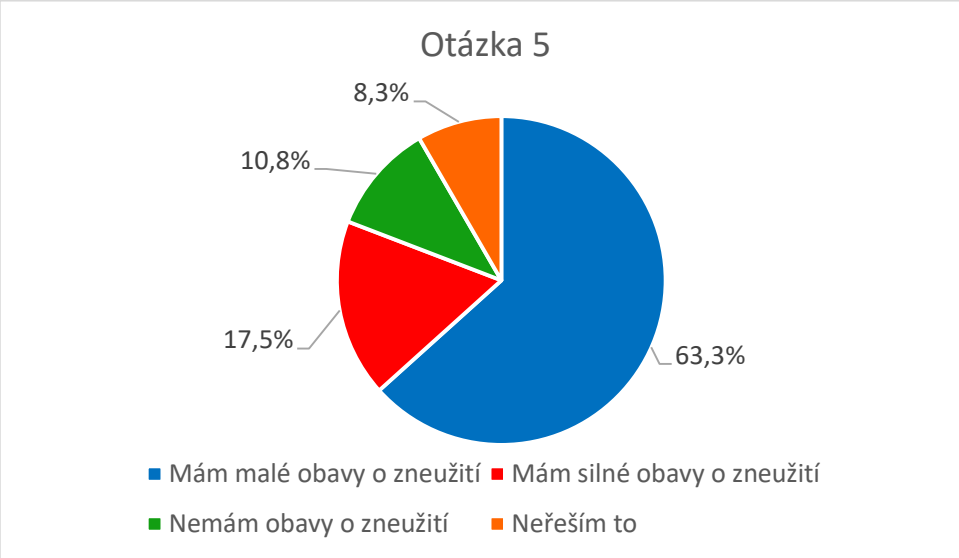


Graf 2: Otázka 4 - Bezpečnost identifikačních dokladů

Zdroj: vlastní zpracování

Otázka 5: Jak se cítíte ohledně možného zneužití osobních informací, které jste poskytli online?

Otázka se zaměřuje na subjektivní vnímání možnosti zneužití osobních online informací respondenty. Tento dotaz má za cíl zhodnotit úroveň obav mezi studenty. Téměř 81 % respondentů vyjádřilo nějakou formu obav ohledně potencionálního zneužití svých osobních informací online. 10,8 % dotázaných nevyjádřilo žádné obavy ohledně zneužití, zatímco 8,3 % odpovědělo, že se tímto problémem nezabývá. Zastupuje prvek „únik soukromých dat," stejně jako otázka 6.

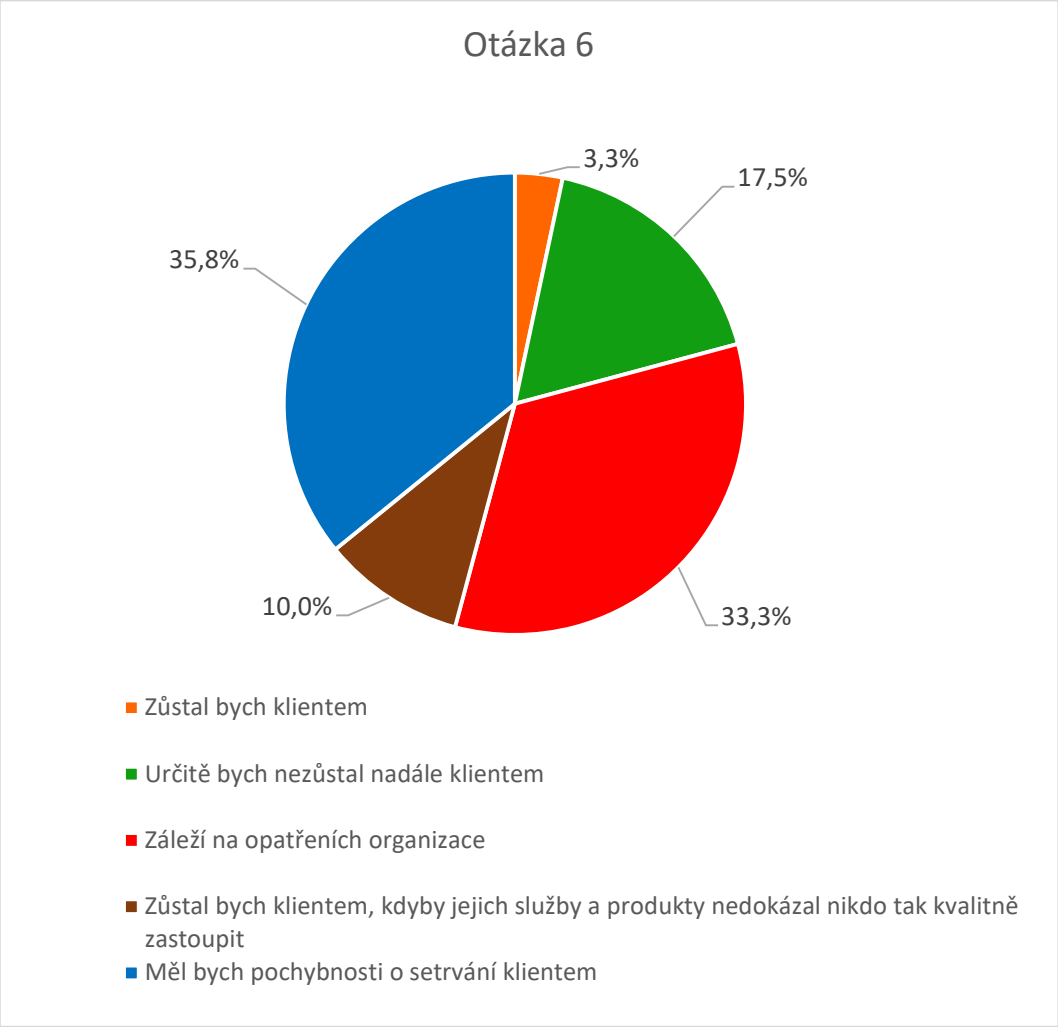


Graf 3: Otázka 5 - Zneužití osobních informací

Zdroj: Vlastní zpracování

Otázka 6: Pokud by došlo k úniku dat z určité organizace, kde máte svůj účet a využíváte jejich služby nebo produkty, zvažovali byste, zda zůstanete jejich klientem?

Tato otázka rozšiřuje téma z otázky 5. Zkoumá, jak by respondenti reagovali v případě úniku jejich osobních informací z určité organizace. Zjišťuje, jaký postup by zvolili. Pouze 3,3 % respondentů by zůstalo klienty dané organizace, zatímco 10 % by setrvalo, pokud by nebylo možné najít kvalitní alternativu. Odpověď „záleží na opatřeních organizace“ zvolilo 33,3 %, což znamená, že by poskytli prostor pro reakci na problémy. 35,8 % respondentů vyjádřilo pochybnosti o setrvání u dané společnosti a rozhodně by s ní nezůstalo 17,5 % dotázaných.

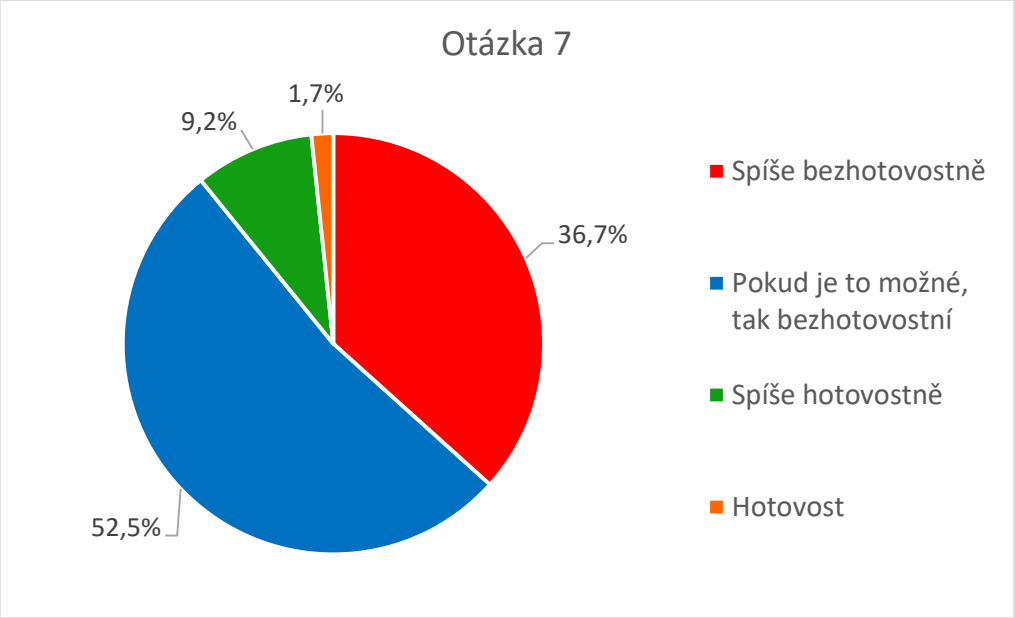


Graf 4: Otázka 6 - Reakce na únik dat z organizace

Zdroj: Vlastní zpracování

Otázka 7: Preferujete bezhotovostní platby nebo platby hotovostí při provádění nákupů?

Otázka zjišťuje poměr použití digitálních a fyzických forem plateb. Z odpovědí vyplývá, že mezi studenty se platba hotovostí téměř vytratila. Pouze 1,7 % respondentů stále preferuje hotovostní platby, 9,2 % uvádí spíše hotovostní platby, zatímco 36,7 % preferuje spíše bezhotovostní platby a 52,5 % uvádí, že se, pokud možno, vyhýbají platbám v hotovosti. Tento trend jasně ukazuje, že pro studenty je platba hotovostí minulostí. Tato otázka a otázka 8 reprezentuje prvek „digitální nástroje."

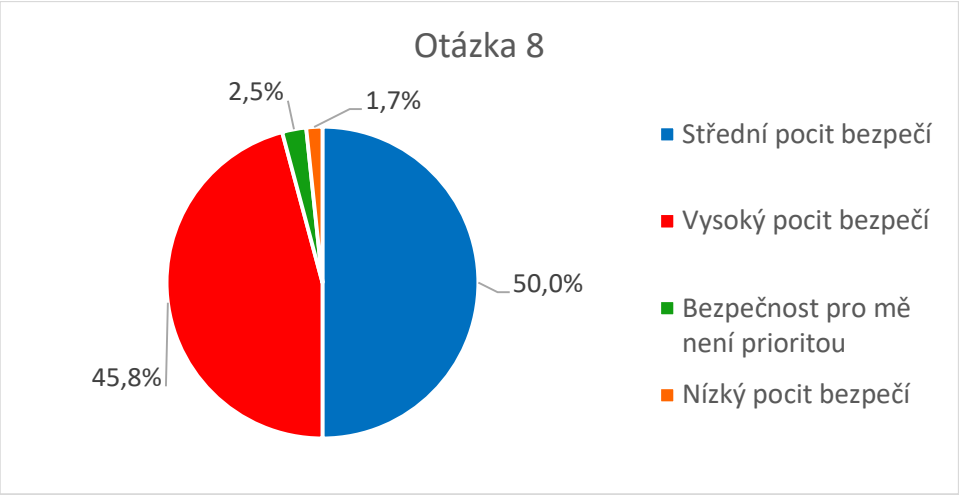


Graf 5: Otázka 7 – Využití bezhotovostních plateb

Zdroj: Vlastní zpracování

Otázka 8: Jak vnímáte bezpečnost bezhotovostních plateb?

V návaznosti na otázku 7 bylo dotazování zaměřeno na vnímání bezpečnosti bezhotovostních plateb. Většina z nich věří těmto platebním metodám a nepociťuje vysoké obavy ohledně bezpečnosti. Vysoký pocit bezpečí vyjádřilo 45,8 % dotázaných, zatímco 50 % odpovědělo, že má střední pocit bezpečí. Nízký pocit bezpečí vyjádřilo pouze 1,7 % respondentů a 2,5 % uvedlo, že pro ně bezpečnost není prioritou.

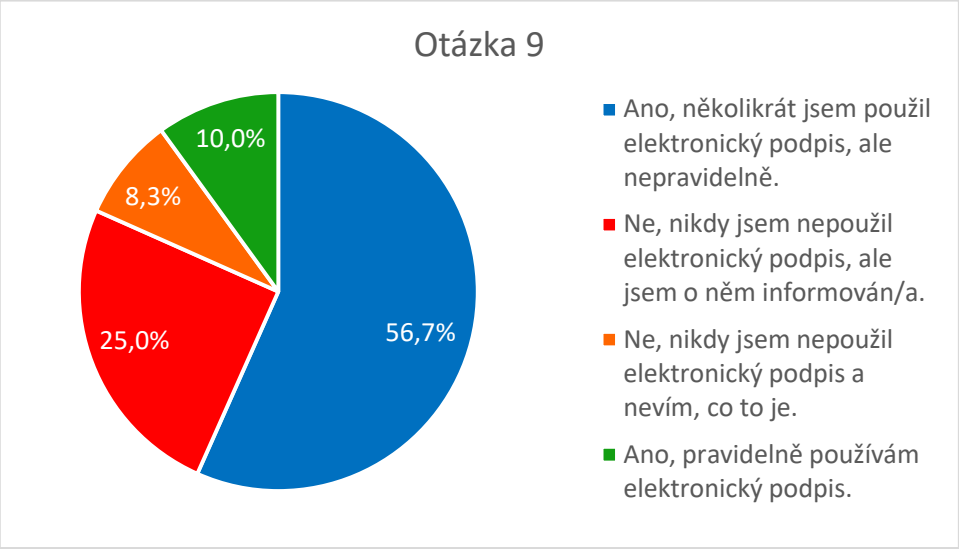


Graf 6: Otázka 8 - Bezpečnost bezhotovostních plateb

Zdroj: Vlastní zpracování

Otázka 9: Použili jste někdy elektronický podpis?

Tato otázka se týkala využívání elektronického podpisu mezi studenty. Jde o digitální nástroj a je součástí prvku „digitální nástroje," který konkuruje tradičnímu ručnímu podpisu na papírových dokumentech. Respondenti měli k dispozici čtyři možné odpovědi. Více než polovina studentů, konkrétně 56,7 %, uvedla, že elektronický podpis používají, ale nepravidelně. Pouze 10 % studentů deklarovalo, že tento nástroj využívají pravidelně. Čtvrtina dotázaných uvedla, že o elektronickém podpisu ví, ale sami ho ještě nepoužili. Menší skupina, přesněji 8,3 %, odpověděla, že o elektronickém podpisu nemají žádné povědomí, a to ani o jeho existenci.



Graf 7: Otázka 9 – Využívání elektronického podpisu

Zdroj: Vlastní zpracování

Otázka 10: Jak často zabezpečujete své účty vícefaktorovým ověřením (např. dvoufaktorová autentizace – SMS kód)?

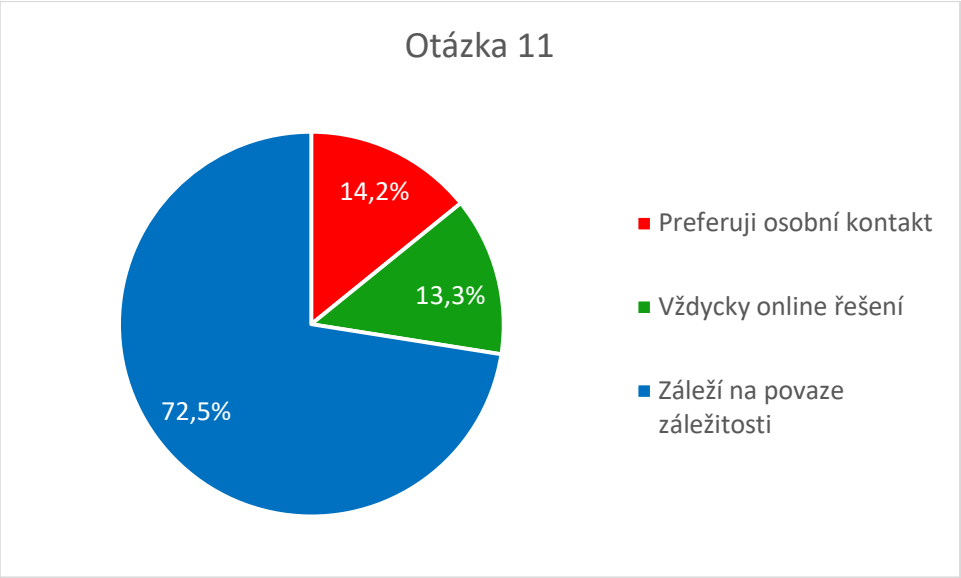
Tato otázka byla začleněna s cílem zjistit, zda studenti aktivně využívají vícefaktorové ověřování na svých účtech jako další vrstvu zabezpečení, která by měla zabránit zneužití jejich osobních účtů. Téměř polovina respondentů, konkrétně 49,2 %, uvedla, že využívají vícefaktorové ověření na citlivých účtech. Na druhém místě podle počtu odpovědí byla možnost „Používám vícefaktorové ověření na všech mých účtech," kterou zvolilo 29,2 % dotázaných. Nejmenší podíl respondentů (21,7 %) uvedl, že používá vícefaktorové ověření pouze tam, kde je vyžadováno. Tato otázka reprezentuje prvek „ochrana účtu."

Graf 8: Otázka 10 - Využívání vícefaktorového ověření

Zdroj: Vlastní zpracování

Otázka 11: V oblasti řešení různých záležitostí, dáváte přednost online řešením, pokud je to možné, nebo upřednostňujete osobní kontakt?

Odpovědi v této otázce poskytují informace o preferencích studentů v řešení různých záležitostí, pokud je možný jak osobní kontakt, tak online řešení. Nejvíce odpovědí zastávala možnost „Záleží na povaze záležitosti," kterou zvolilo 72,5 % respondentů. To znamená, že studenti si uvědomují, že osobní kontakt nemusí být vždy nezbytný a online řešení může být vhodnější. Menší skupina respondentů projevila sklony k osobnímu kontaktu (14,2 %), zatímco jen 13,3 % respondentů vždy upřednostňuje online řešení. Většina studentů tedy neupřednostňuje plně online řešení ve všech záležitostech. Ačkoli byla možnost „Nemám preference" zahrnuta, žádný z respondentů tuto možnost nevybral. Jedná se o prvek „Online řešení záležitosti."

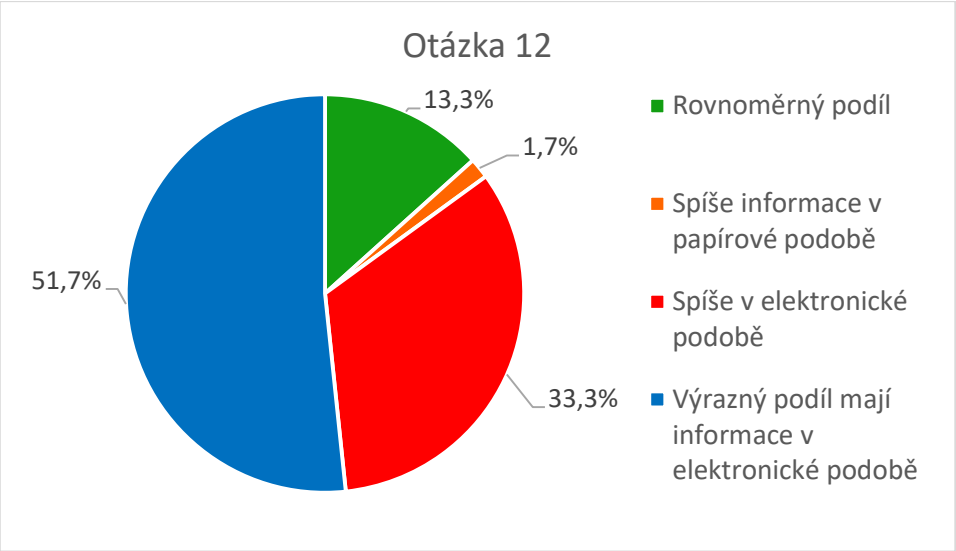


Graf 9: Otázka 11 - Preference online řešení záležitosti nebo osobní kontakt

Zdroj: Vlastní zpracování

Otázka 12: Získáváte častěji informace z elektronických zdrojů nebo tištěných zdrojů (knihy, časopisy atd.)?

Podle výsledků je zřejmé, že elektronická forma získávání informací má výraznou převahu. Většina studentů (51,7 %) upřednostňuje elektronický způsob získávání informací, zatímco 33,3 % se vyjádřilo, že spíše získává informace v elektronické podobě. Skupina o velikosti 13,3 % vyjadřuje rovnoměrný zájem o obě formy získávání informací, zatímco pouze 1,7 % preferuje spíše papírovou podobu. Žádný respondent neupřednostnil výrazně papírový způsob. Tyto výsledky jasně signalizují silnou preferenci studentů pro elektronický způsob získávání informací. Tato otázka reprezentuje prvek „zisk informací," stejně jako otázka 13.

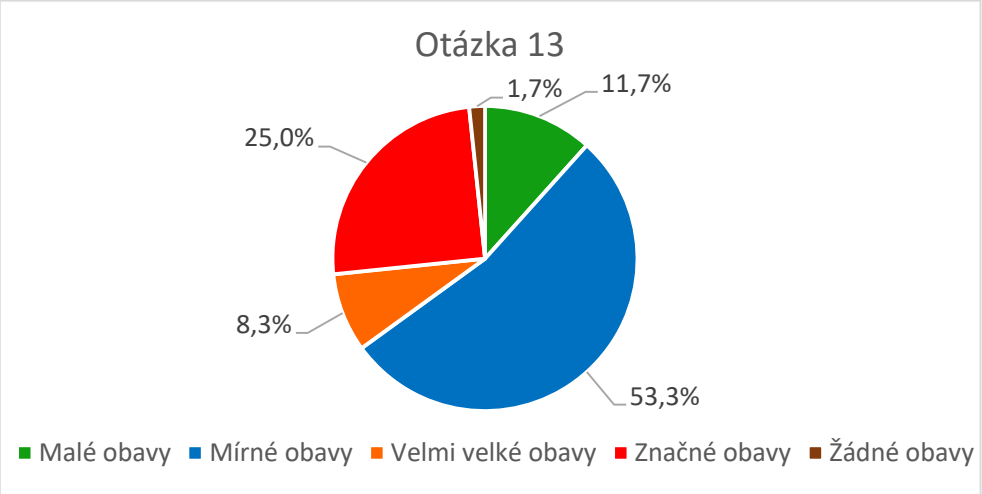


Graf 10: Otázka 12 - Preference elektronických zdrojů nebo tištěných

Zdroj: Vlastní zpracování

Otázka 13: Jak moc velké obavy máte z toho, že získané informace v digitální formě mohou být falešné nebo zavádějící?

Tato otázka rozvíjí téma předchozí otázky. Zkoumá obavy ohledně autentičnosti digitálně získaných informací. Největší část respondentů (53,3 %) vyjádřila mírné obavy, což naznačuje, že existuje určitá opatrnost při získávání informací. Značná část (25 %) má výrazné obavy a 11,7 % respondentů uvedlo malé obavy. Pouze malý počet respondentů (8,3 %) projevil velké obavy a minimální část (1,7 %) nevyjádřila žádné obavy. Tyto výsledky naznačují, že studenti jsou si vědomi možného výskytu falešných informací a projevují v této souvislosti určitou míru obezřetnosti.

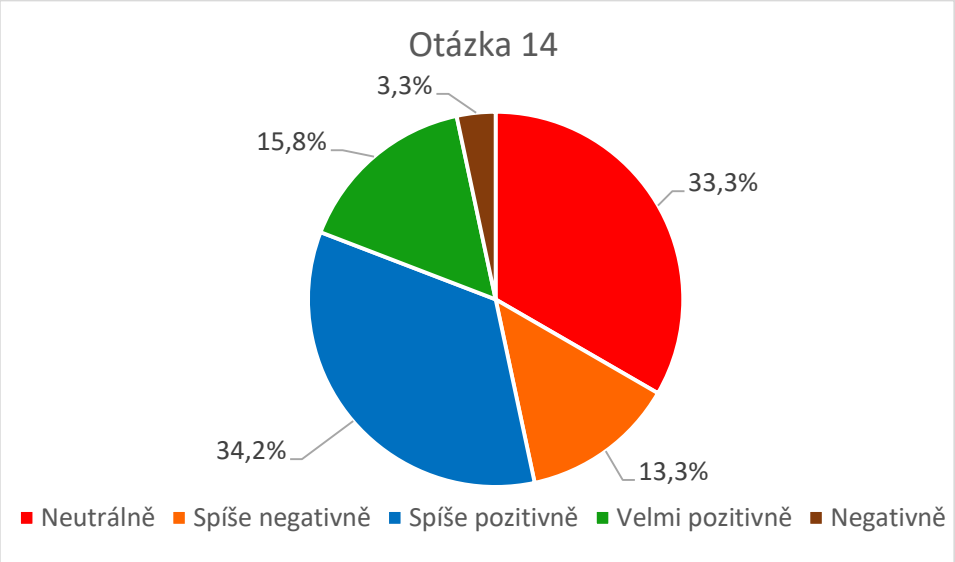


Graf 11: Otázka 13 - Obavy z hlediska falešnosti informací v digitální formě

Zdroj: Vlastní zpracování

Otázka 14: Jak vnímáte trend implementace umělé inteligence do různých aspektů života (digitální asistenti (např. Siri), autonomní řízení, CHATGPT atd.)

Otázka zkoumala názory respondentů na umělou inteligenci a její postupnou implementaci do různých oblastí života. Nejvíce z nich (34,2 %) tuto integraci vnímá spíše pozitivně, přičemž 15,8 % z celkového počtu ji dokonce považuje za velmi pozitivní trend. Pouze menší skupina respondentů má negativnější názor – 13,3 % vyjádřilo spíše negativní postoj a pouhých 3,3 % má zcela negativní stanovisko. Neutrální přístup zaujímá 33,3 % studentů. Z výsledků vyplývá, že většina studentů nevidí v rozvoji umělé inteligence zásadní problém. Otázka reprezentuje prvek „umělá inteligence," stejně jako otázka 15.

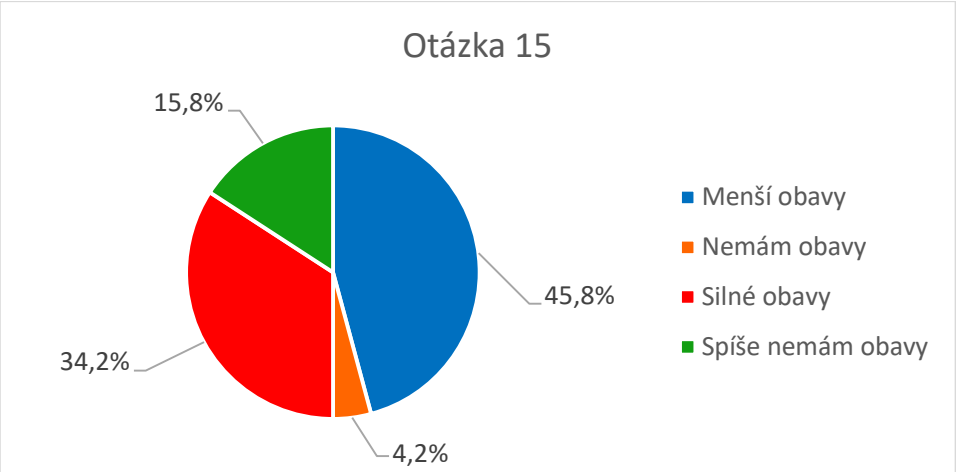


Graf 12: Otázka 14 - Vnímání trendu implementace umělé inteligence

Zdroj: Vlastní zpracování

Otázka 15: Máte obavy z využívání umělé inteligence k šíření dezinformací a fake news?

Navazuje na otázku 14, představující pokračování v rámci problematiky zkoumání postojů respondentů k umělé inteligenci. Soustředí se na zjištění míry obav využití umělé inteligence k šíření dezinformací a falešných zpráv. Pouze menší část respondentů (15,8 %) v této souvislosti spíše nemá obavy a 4,2 % uvedlo, že nemá vůbec žádné obavy. Naopak, největší část studentů (45,8 %) má mírné obavy a značná část z nich (34,2 %) projevuje silné obavy. Výsledky této otázky naznačují, že respondenti si jsou vědomi možného využití umělé inteligence v šíření dezinformací a falešných zpráv.



Graf 13: Otázka 15 – Obavy z využívání umělé inteligence k šíření dezinformací

Zdroj: Vlastní zpracování

7.5 Test nezávislosti

Byly zamýšleny dva testy nezávislosti, první test nezávislosti se zaměřuje na otázky 2 a 3. Druhý test se zaměřuje na pohlaví a otázku 10.

Důvodem pro první test je zjištění, jestli existuje spojitost mezi informovaností o aplikaci a ochotou ji používat.

Důvodem pro druhý test je zjištění, jestli obě pohlaví mají podobně stejnou tendenci využívat vícefaktorové ověření.

V této kapitole byl použit Chí-kvadrát test nezávislosti v kontingenční tabulce. Jedná se o statistickou metodu k ověření nezávislosti mezi dvěma kategoriálními proměnnými. Pro použití tohoto testu existují dvě základní podmínky: [61]

- Podíl očekávaných četností menších než 5 nesmí překročit 20%
- Žádná z očekávaných četností nesmí být menší než 2

Použitý vzorec:

$$\chi^2 = \sum_{i=1}^{r}\sum_{j=1}^{c} \frac{\left(n_{ij} - \frac{n_{i.}n_{.j}}{n}\right)^2}{\frac{n_{i.}n_{.j}}{n}}$$

Obrázek 8: Chí-kvadrát vzorec

Zdroj: https://www.geoinformatics.upol.cz/dprace/bakalarske/papakova10/testy.html

Veškerá data jsou získána z dotazníkového šetření a k tvorbě výsledků byl použit software Microsoft Excel. Testováno na hladině významnosti alfa = 0,05.

7.5.1 Test nezávislosti mezi otázkou 2 a 3

Tento test je zaměřen na zjištění, zda existuje statisticky významná závislost mezi povědomím respondentů o mobilní aplikaci eDoklady a jejich plánovanému používání. Cílem je analyzovat, jestli předešlá znalost aplikace ovlivňuje sklon jednotlivců k jejímu možnému budoucímu používání.

Hypotézy:

- H_0: Neexistuje závislost mezi povědomím o mobilní aplikaci a jejich plánovanému využívání
- H_1: Existuje závislost mezi povědomím o mobilní aplikaci a jejich plánovanému využívání

Nejprve byla vytvořena kontingenční tabulka a zkopírovány hodnoty, aby s daty bylo možno jednodušeji pracovat.

Počet z 2. otázka	Třetí otázka - sloupec				
Druhá otázka - řádek	Ne	Ano	Spíše ano	Spíše ne	Celkový součet
Ne	5	14	20	20	59
Ano	3	26	23	9	61
Celkový součet	**8**	**40**	**43**	**29**	**120**

Skutečné četnosti					
Počet z 2. otázka	Třetí otázka - sloupec				
Druhá otázka - řádek	Ne	Ano	Spíše ano	Spíše ne	Celkový součet
Ne	5	14	20	20	59
Ano	3	26	23	9	61
Celkový součet	8	40	43	29	120

Obrázek 9: Kontingenční tabulka

Zdroj: Vlastní zpracování

Dalším krokem bylo spočítání **očekávaných četností** podle vzorce a ověření splnění podmínky. 20 % z 8 buněk se rovná hodnotě 1,6. Je tedy možné mít maximálně 1 buňku pod hodnotou 5. Tato podmínka nebyla splněna. Následovalo sloučení kategorií. Kategorie „Ne“ a „Spíše ne“ byly sloučeny dohromady. Podmínka byla splněna.

Výsledek je zde:

Skutečné četnosti				
Počet z 2. otázka	Třetí otázka - sloupec			
Druhá otázka - řádek	Ano	Spíše ano	Spíše ne	Celkový součet
Ne	14	20	25	59
Ano	26	23	12	61
Celkový součet	40	43	37	120
ni.n.j/n				
Počet z 2. otázka	Třetí otázka - sloupec			
Druhá otázka - řádek	Ano	Spíše ano	Spíše ne	Celkový součet
Ne	19,666667	21,14166667	18,19166667	59
Ano	20,333333	21,85833333	18,80833333	61
Celkový součet	40	43	37	120

Obrázek 10: Očekávané četnosti

Zdroj: Vlastní zpracování

Posledním krokem pro vypočítání testovací statistiky byla finalizace celého vzorce. Testovací statistika byla vypočítána vzorcem Suma z celé tabulky hodnot. Stupně volnosti se vypočítají jako (r-1) * (s-1). Výsledek testovací statistiky je označeno tučně.

χ^2			
Počet z 2. otázka	Třetí otázka - sloupec		
Druhá otázka - řádek	Ano	Spíše ano	Spíše ne
Ne	1,632768362	0,0616509	2,548056955
Ano	1,579234973	0,059629559	2,464514104
Celkový součet			
r	2	r-1	1
s	3	s-1	2
Testovací statistika	**8,345854853**		

Obrázek 11: Výpočet hodnoty testovací statistiky

Zdroj: Vlastní zpracování

Díky výpočtu stupně volnosti byla pomocí funkce CHISQ.INV zjištěna kritická hodnota. Stanovení hypotézy záviselo na tom, zda hodnota testovací statistiky je větší nebo menší než uvedená kritická hodnota.

(r-1) * (s-1)	2
alpha	0,05
chí_0,95(2)	**5,991464547**
Kritická hodnota	5,991
	H0 zamítám a přijímám H1

Obrázek 12: Výsledek testu nezávislosti mezi otázkou 2 a 3

Zdroj: Vlastní zpracování

Testovací statistika **(8,345854853)** je větší než 5,991. To znamená, že hypotéza H_0 se nepotvrdila a je tedy zamítnuta, tím pádem H_1 mohla být přijata. Výsledkem analýzy je existence závislosti mezi povědomím o mobilní aplikaci a jejím plánovaným využíváním.

7.5.2 Test nezávislosti mezi pohlavím a otázkou 10

Předmětem tohoto zkoumání je existence statisticky významné závislosti mezi pohlavím a odpověďmi na otázku: „Jak často zabezpečujete své účty vícefaktorovým ověřením (např. dvoufaktorová autentizace – SMS kód)?“

Stanovené hypotézy:

- H_0: Neexistuje závislost mezi pohlavím respondentů a způsobem zabezpečení účtů pomocí vícefaktorového ověření
- H_1: Existuje závislost mezi pohlavím respondentů a způsobem zabezpečení účtů pomocí vícefaktorového ověření

Způsob vypracování je podobný jako v kapitole 7.5.1. Odpovědi na otázku 10 byly zakódovány následovně:

- Používám vícefaktorové ověření na citlivých účtech (např. účty s penězi, citlivými informacemi, sociálními sítěmi) = **1**
- Používám vícefaktorové ověření na všech svých účtech = **2**
- Používám vícefaktorové ověření pouze tam, kde je vyžadováno, jinak ne = **3**

Podmínka chí-kvadrát testu zapříčinila vymazání kategorie „Jiné“. Následný postup probíhal stejně jako předešlý.

Skutečné a očekávané četnosti:

Počet z Pohlaví	Popisky sloupců			
Popisky řádků	**1**	**2**	**3**	**Celkový součet**
Jiné	1			1
Muž	34	20	15	69
Žena	24	15	11	50
Celkový součet	**59**	**35**	**26**	**120**

Skutečné četnosti				
Počet z Pohlaví	Popisky sloupců			
Popisky řádků	1	2	3	Celkový součet
Muž	34	20	15	69
Žena	24	15	11	50
Celkový součet	58	35	26	119

ni.n.j/n				
Počet z Pohlaví	Popisky sloupců			
Popisky řádků	1	2	3	Celkový součet
Muž	33,6302521	20,294	15,076	69
Žena	24,3697479	14,706	10,924	50
Celkový součet	58	35	26	119

Obrázek 13: Skutečné a očekávané četnosti

Zdroj: Vlastní zpracování

Dále byl finalizován vzorec a vypočítána testovací statistika a kritická hodnota. Výsledek testovací statistiky je **0,0207231.** Kritická hodnota je 5,991.

r	2	r-1	1
s	3	s-1	2
Testovací statistika	**0,0207231**		
(r-1) * (s-1)	2		
alpha	0,05		
chí_0,95(2)	**5,991464547**		
Kritická hodnota	5,991		
	H0 nemůžu zamítnout		

Obrázek 14: Výsledek testu nezávislosti mezi pohlavím a otázkou 10

Zdroj: Vlastní zpracování

Tento výsledek značí, že nulovou hypotézu nelze zamítnout. Znamená to, že se nemůže potvrdit existence statisticky významného vztahu mezi pohlavím respondentů a zabezpečení účtu pomocí vícefaktorového ověření. Muži i ženy měli podobné návyky.

7.6 Vyhodnocení dotazníku

Cílem tohoto výzkumu bylo provést analýzu digitální důvěry s ohledem na její komplexní charakter zasahující do mnoha oborů a následně zkoumat, jak tato specifická forma důvěry ovlivňuje postoje jednotlivců k otázkám v oblasti digitální bezpečnosti, ochrany osobních údajů a jejich názorů na umělou inteligenci v souladu s uvedenými prvky digitální důvěry.

Podle počtu a způsobu odpovědí na první otázku lze konstatovat, že studenti mají obecné povědomí o termínu digitální důvěra a jsou schopni spojit oblasti, kde se tato forma důvěry uplatňuje.

Zhruba polovina respondentů má povědomí o aplikaci eDoklady a 69 % studentů vyjadřuje otevřenost k využívání digitálních identifikačních dokladů. Avšak pouze 20 % studentů projevuje větší důvěru v digitální formu než ve fyzické prvky, pokud jde o bezpečnost. Celkově lze pozorovat, že studenti jsou nakloněni možnosti digitalizace identifikačních dokladů. Zároveň preferují fyzickou formu kvůli bezpečnostním aspektům, což indikuje, že studenti by se pravděpodobně rozhodli používat tuto aplikaci kvůli centralizaci dokladů a snadnějšímu využívání, spíše než kvůli bezpečnosti.

Prvek „únik soukromých dat“ byl tvořen otázkami 5 a 6. Skoro 81 % respondentů vyjadřuje obavy ohledně možného zneužití svých osobních informací. Pouze 13,3 % uvažovalo o zůstání klientem při úniku dat z organizace, zatímco 33,3 % by v této situaci čekalo na reakci organizace. Zbytek by měl vážné pochybnosti o zůstání klientem. Tyto výsledky značí, že studenti jsou citliví na únik dat, ale při správné reakci organizace by byli ochotni zůstat klienty.

Dalším prvkem jsou digitální nástroje, zkoumané primárně prostřednictvím otázek 7, 8 a 9. Použití hotovosti mezi studenty je téměř zanedbatelné s pouhými 1,7 %. Bezhotovostní platby jsou preferované a většinou studentů považovány za bezpečné. Dále se práce věnuje využívání elektronického podpisu, kde výsledky ukazují, že jeho používání není příliš běžné. Celkově lze pozorovat, že studenti jsou otevřeni používání

digitálních nástrojů, mají zájem o digitální identifikační doklady a více než polovina respondentů již využila elektronický podpis.

Prvek ochrany účtu je reprezentován otázkou 10. Přibližně polovina studentů využívá vícefaktorové zabezpečení na citlivých účtech a 29,2 % na všech účtech. To nasvědčuje snaze posílit bezpečnost a znesnadnit případné narušení. Menšinu tvoří studenti používající vícefaktorové ověření jen když musí, což může být chápáno jako minimalizování obtížnosti a zdlouhavosti procesu ověřování. Celkově tyto výsledky naznačují, že studenti kladou důraz na ochranu svých účtů.

Otázka 11 zastupuje prvek „preference v řešení záležitostí." Většina respondentů upřednostňuje flexibilitu, kdy volba řešení situace závisí na povaze konkrétní situace. To naznačuje, že ne vždy považují osobní kontakt za nezbytný a upřednostní online řešení.

Dalším prvkem je zisk informací tvořený otázkami 12 a 13. Výsledky jasně ukazují, že studenti dávají přednost elektronickým informačním zdrojům před tištěnými. Zároveň mají obavy ohledně věrohodnosti těchto informací a uvědomují si, že daná zpráva může být falešná. Tyto obavy by měly vést ke kritickému myšlení a k odhalení potencionálního rizika.

Posledním prvkem je umělá inteligence tvořena otázkami 14 a 15. Z výsledků vyplývá, že mnoho studentů (50 %) vnímá tento trend pozitivně nebo velmi pozitivně. Neutrální stanovisko zaujímá 33 % studentů. To ukazuje otevřenost k dalšímu vývoji a implementaci umělé inteligence do různých aspektů života. Zároveň si studenti uvědomují možnost využití AI k tvoření a šíření dezinformací a fake news. I přesto, že menšina vyjádřila svůj názor negativně, je zřejmé, že si studenti uvědomují potencionální negativní aspekty a rizika spojená s implementací umělé inteligence.

Dále byly vytvořeny 2 testy nezávislosti. První test zjistil existenci statisticky významné závislosti mezi povědomím o mobilní aplikaci eDoklady a jejím plánovaným využíváním. Druhý test zkoumal možnou závislost mezi pohlavím respondentů a způsobem zabezpečení účtů pomocí vícefaktorového ověření. Zde výsledek nepotvrdil hypotézu, mezi těmito prvky tedy neexistuje statisticky významná závislost.

Celkově studenti projevují obecný přehled o pojmu digitální důvěra a jsou otevřeni používání digitálních technologií a implementace umělé inteligence.

7.7 Zhodnocení výzkumu

Celkový počet odpovědí překročil původně plánovaný počet respondentů. Výzkum zjistil, co si respondenti představují pod pojmem digitální důvěra, jaké mají postoje v uvedených oblastech cíle průzkumu z hlediska zakomponovaných prvků. Tyto poznatky vedly k dosažení stanoveného cíle průzkumu.

Studenti byli vybráni z oborů technických i netechnických, přičemž respondenti byli zhruba rovnoměrně rozděleni mezi pět oslovených fakult. Bylo to tak zamýšleno, aby odpovědi rovnoměrně pokrývaly postoje studentů. Odpovědi byly proto vyhodnocovány jako celek, tedy jako postoj „průřezového" studenta. Nicméně bych doporučil pro případné návazné zpracování také vyhodnotit, jak např. reagují studenti oborů technických a jak oborů netechnických.

Výběr respondentů v této práci umožňuje další výzkum napříč generacemi. Rozšíření výzkumu na starší populaci by umožnilo porovnat a analyzovat rozdíly ve vnímání digitální důvěry a postojů k jednotlivým aspektům mezi studenty a staršími jedinci. Takové srovnání by nabídlo užitečné poznatky ohledně jejich interakce s digitálním prostředím. Doporučil bych přidání otázky rozšiřující téma digitálních identifikačních dokladů, která by jasně objasnila motivaci používání aplikace. Získané výsledky indikovaly používání spíše k centralizaci dokladů a snadnému využívání než kvůli bezpečnosti.

Závěr

Rychlý vývoj digitálních technologií v posledních letech přináší éru, kdy se každodenní životy stávají stále více propojenými s digitálním prostředím přinášejícím zjednodušení, rychlost a efektivitu. Základním vztahem mezi jednotlivcem a digitálním prostředím je důvěra. Důvěra v digitálním světě zahrnuje povědomí o tom, že veškeré naše informace jsou v bezpečí a že máme kontrolu nad tím, jak jsou naše osobní údaje používány. Jedná se o jeden z prvků digitální důvěry, ale jedná se o daleko komplexnější téma, kdy nejde jen o technologie, ale také o postoje, preference a znalosti jednotlivců.

Bakalářská práce se zaměřila na rozbor pojmu „digitální důvěra“ a jeho různých aspektů. To zahrnovalo zkoumání obecného termínu důvěry, fyzickou důvěru v kontextu digitálního prostředí příkladem digitálních identifikačních dokladů, obecnou bezpečnost s ohledem na různé hrozby, jako jsou hackerské útoky a podvody, a zkoumání možnosti ochrany účtu skrze vícefaktorové ověření. Dále byly popsány digitální nástroje, které mohou konkurovat fyzickým ekvivalentům, například elektronický podpis. Dále byl zkoumán i jeden z aktuálně nejvíce rozvíjejících se aspektů, a to umělá inteligence, kde bylo vyzkoušeno, jak jednoduché je vytvořit dezinformaci pomocí ChatGPT. Vycházejíc ze zkoumání těchto aspektů byly vybrány prvky do dotazníkového průzkumu a následně byly integrovány do otázek pro zjištění názorů a přístupu respondentů k těmto prvkům, týkající se komplexní problematiky digitální důvěry.

Dotazníkový průzkum byl zaměřen výhradně na studenty Univerzity Pardubice. Výsledky byly získané z různých fakult, přičemž na každé fakultě se pracuje s odlišnými technologiemi. Nejen samotný charakter fakult, ale i individuální přístup studentů k digitálním úkonům je odlišný, což ovlivňuje názory a postoje k různým aspektům digitální důvěry. Bylo zjištěno, že respondenti mají schopnost si představit, co znamená pojem digitální důvěra, projevují obavy ohledně bezpečnosti svých osobních údajů, avšak tyto obavy nejsou nadměrné. Zároveň projevují otevřenost vůči využívání digitálních technologií a implementaci umělé inteligence.

Nejvíce mě překvapily výsledky souvisejících otázek ohledně záměru využívání mobilní aplikace eDoklady a preference ohledně bezpečnosti digitální formy oproti fyzickému prvku. Ukázalo se, že 69 % respondentů uvažuje o používání aplikace, ale pouze 20 % považuje digitální formát za bezpečnější. Tvůrcům aplikace bych

doporučil rozsáhlejší informování veřejnosti ohledně bezpečnosti ve srovnání s fyzickými prvky.

Výběr respondentů umožňuje pokračování výzkumu i u jiných věkových skupin. Současně existuje možnost zaměřit se výhradně na studenty technických nebo netechnických oborů.

Použitá literatura

[1] The Meanings of Trust. ResearchGate [online]. 1996 [cit. 2023-11-28]. Dostupné z: https://www.researchgate.net/publication/239538703_The_Meanings_of_Trust

[2] Trust: What It Is And What It Is Not. ResearchGate [online]. 2003 [cit. 2023-11-28]. Dostupné z: https://www.researchgate.net/publication/297891579_Trust_What_It_Is_And_What_It_Is_Not

[3] Evocable Trust. Psychology Today [online]. 2018 [cit. 2023-11-28]. Dostupné z: https://www.psychologytoday.com/us/blog/one-among-many/201811/evocable-trust

[4] Not So Different After All: A Cross-discipline View of Trust. ResearchGate [online]. 1998 [cit. 2023-11-28]. Dostupné z: https://www.researchgate.net/publication/50313187_Not_So_Different_After_All_A_Cross-discipline_View_of_Trust

[5] Osobní doklady. Ministerstvo vnitra České republiky [online]. c2023 [cit. 2023-11-28]. Dostupné z: https://www.mvcr.cz/clanek/osobni-doklady-642319.aspx?q=Y2hudW09Mg%3D%3D

[6] Pas 92 tisíc, občanka 28 tisíc korun. Falešné české doklady patří k nejdražším. Novinky.cz [online]. 2022 [cit. 2023-11-28]. Dostupné z: https://www.novinky.cz/clanek/domaci-pas-92-tisic-obcanka-28-tisic-korun-falesne-ceske-doklady-patri-k-nejdrazsim-40403110

[7] Biometrický cestovní pas. Velvyslanectví České republiky v Tiraně [online]. [cit. 2023-11-28]. Dostupné z: https://www.mzv.cz/tirana/cz/viza_a_konzularni_informace/cestovni_doklady/biometricky_cestovni_pas/index.html

[8] Programové prohlášení vlády. Vláda České republiky [online]. 2023 [cit. 2023-11-28]. Dostupné z: https://www.vlada.cz/cz/programove-prohlaseni-vlady-193547/#digitalizace

[9] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY. Evropská komise [online]. 2021 [cit. 2023-11-28]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52021PC0281&from=EN

[10] Nová éra prokazování totožnosti? Už brzy. EDoklady [online]. 2023 [cit. 2023-11-28]. Dostupné z: https://edoklady.gov.cz

[11] What are the benefits of eID? European Commission [online]. [cit. 2023-11-28]. Dostupné z: https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Benefits+of+eID

[12] Pros and Cons of Digital ID Card | Advantages and Disadvantages of Digital ID Card. Pros Cons [online]. 2023 [cit. 2023-11-28]. Dostupné z: https://www.proscons.info/2023/03/pros-and-cons-of-digital-id-card.html#gsc.tab=0

[13] Number of internet and social media users worldwide as of October 2023. Statista [online]. 2023 [cit. 2023-11-28]. Dostupné z: https://www.statista.com/statistics/617136/digital-population-worldwide/

[14] Earning Digital Trust: Decision-Making for Trustworthy Technologies. World economic forum [online]. 2022 [cit. 2023-11-28]. Dostupné z: https://www.weforum.org/publications/earning-digital-trust-decision-making-for-trustworthy-technologies/

[15] KAUSHIK, Pal. Digital Trust. Techopedia [online]. 2023 [cit. 2023-11-28]. Dostupné z: https://www.techopedia.com/definition/33932/digital-trust

[16] RITTER, Jeffrey. Digital trust. WhatIs.com [online]. 2019 [cit. 2023-11-28]. Dostupné z: https://www.techtarget.com/whatis/definition/digital-trust

[17] Earning Digital Trust: Decision-Making for Trustworthy Technologies. World economic forum [online]. 2022 [cit. 2023-11-28]. Dostupné z: https://www3.weforum.org/docs/WEF_Earning_Digital_Trust_2022.pdf

[18] CHIN, Kyle. Biggest Data Breaches in US History [Updated 2023]. UpGuard [online]. 2023 [cit. 2023-11-28]. Dostupné z: https://www.upguard.com/blog/biggest-data-breaches-us

[19] Building digital trust: Technology can lead the way. DELOITTE. Deloitte Insights [online]. 2023 [cit. 2023-11-28]. Dostupné z: https://www2.deloitte.com/content/dam/insights/us/articles/6320_Building-digital-trust/DI_Building-digital-trust.pdf

[20] VW installed 'defeat devices' to subvert emissions tests, high court finds. The Guardian [online]. 2020 [cit. 2023-11-28]. Dostupné z: https://www.theguardian.com/business/2020/apr/06/volkswagen-installed-thousands-unlawful-defeat-devices-high-court-dieselgate

[21] How Do Businesses Use Artificial Intelligence?court finds. Wharton Online [online]. 2020 [cit. 2023-11-28]. Dostupné z: https://online.wharton.upenn.edu/blog/how-do-businesses-use-artificial-intelligence/

[22] 5 things you need to know about Data Privacy [Definition & Comparison]. Data Privacy Manager [online]. 2023 [cit. 2023-11-28]. Dostupné z: https://dataprivacymanager.net/5-things-you-need-to-know-about-data-privacy/

[23] DESHPANDE, Indrajeet. What Is Customer Data? Definition, Types, Collection, Validation and Analysis. Spiceworks [online]. 2021 [cit. 2023-11-28]. Dostupné z: https://www.spiceworks.com/marketing/customer-data/articles/what-is-customer-data/

[24] Privacy Policy. Google Privacy & Terms [online]. 2023 [cit. 2023-11-28]. Dostupné z: https://policies.google.com/privacy?hl=en-US#infochoices

[25] What is the CIA triad (confidentiality, integrity and availability)? WhatIs.com [online]. 2023 [cit. 2023-11-28]. Dostupné z: https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

[26] 14 Pros and Cons of Digital Technology. Honest Pros and Cons [online]. 2022 [cit. 2023-11-28]. Dostupné z: https://honestproscons.com/pros-and-cons-of-digital-technology/

[27] 21 Advantages and Disadvantages of Digital Technology. Yo cover [online]. 2022 [cit. 2023-11-28]. Dostupné z: https://yocover.com/advantages-and-disadvantages-of-digital-technology/

[28] 7 benefits of automation for your business, with examples. Mondayblog [online]. 2022 [cit. 2023-11-28]. Dostupné z: https://monday.com/blog/business-administration/benefits-of-automation/

[29] What Are The Benefits Of Travel Technology. Technology & Travel - Alertify [online]. [cit. 2023-11-28]. Dostupné z: https://alertify.eu/what-are-the-benefits-of-travel-technology/

[30] Bankovních poboček rychle ubývá. Lidé chtějí vše vyřešit on-line. Banky.cz [online]. 2022 [cit. 2023-11-28]. Dostupné z: https://www.banky.cz/clanky/bankovnich-pobocek-rychle-ubyva-lide-chteji-vse-vyresit-on-line/

[31] The Advantages and Disadvantages of Electronic Banking. SoFi [online]. 2022 [cit. 2023-11-28]. Dostupné z: https://www.sofi.com/learn/content/electronic-banking-advantages-and-disadvantages/

[32] Benefits of E-Banking. Unacedemy [online]. c2023 [cit. 2023-11-28]. Dostupné z: https://unacademy.com/content/bank-exam/study-material/general-awareness/benefits-of-e-banking/

[33] Bezhotovostní platba. Home Credit [online]. c2023 [cit. 2023-11-28]. Dostupné z: https://www.homecredit.cz/slovnik-pojmu/bezhotovostni-platba

[34] A complete guide on the advantages of ecommerce to business. Amazon [online]. c2023 [cit. 2023-11-28]. Dostupné z: https://sell.amazon.in/seller-blog/advantages-of-ecommerce

[35] E-Commerce: Advantages and Limitations. Semantic scholar [online]. c2023 [cit. 2023-11-28]. Dostupné z: https://www.semanticscholar.org/paper/E-Commerce%3A-Advantages-and-Limitations-Taher/1cb49e2ef7c8b63359e98d8d0df78dd13b03943d?p2df

[36] 17 Disadvantages of Digital Technology. Turbo Future [online]. 2023 [cit. 2023-11-28]. Dostupné z: https://turbofuture.com/misc/Disadvantages-of-Digital-Technology

[37] Why We Should All Be Concerned About Digital Privacy. University of California Press [online]. 2023 [cit. 2023-11-28]. Dostupné z: https://www.ucpress.edu/blog/60226/why-we-should-all-be-concerned-about-digital-privacy/

[38] Fake news? Disinformation in the age of digital media. Universität Münster [online]. 2023 [cit. 2023-11-28]. Dostupné z: https://www.uni-muenster.de/news/view.php?cmdid=9428)

[39] Hacker. TechTarget [online]. 2021 [cit. 2023-11-28]. Dostupné z: https://www.techtarget.com/searchsecurity/definition/hacker

[40] KOLOUCH, Jan. CyberCrime [online]. Edice CZ.NIC, 2017 [cit. 2023-11-28]. ISBN 78-80-88168-15-7. Dostupné z: https://www.bookport.cz/kniha/cybercrime-5994/

[41] ESignature. European Commission [online]. [cit. 2023-11-28]. Dostupné z: https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eSignature

[42] Certifikáty a elektronické podpisy v kostce. Sefira [online]. 2021 [cit. 2023-11-28]. Dostupné z: https://www.sefira.cz/blog/prehled-certifikatu-a-typu-elektronickych-podpisu-v-kostce/

[43] EIDAS a elektronické podpisy: jak poznáme, o jaký podpis jde? Lupa.cz [online]. 2021 [cit. 2023-11-28]. Dostupné z: https://www.lupa.cz/clanky/eidas-a-elektronicke-podpisy-jak-pozname-o-jaky-podpis-jde/

[44] Elektronická pečeť dle eIDAS – jak a co vlastně pečetit? Epravo.cz [online]. 2016 [cit. 2023-11-28]. Dostupné z: https://www.epravo.cz/top/clanky/elektronicka-pecet-dle-eidas-jak-a-co-vlastne-pecetit-111613.html

[45] Kvalifikované elektronické pečeti: bude čím je vytvářet? Lupa.cz [online]. 2018 [cit. 2023-11-28]. Dostupné z: https://www.lupa.cz/clanky/kvalifikovane-elektronicke-peceti-bude-cim-je-vytvaret/

[46] Časová razítka. Česká pošta [online]. c2023 [cit. 2023-11-28]. Dostupné z: https://www.ceskaposta.cz/sluzby/certifikacni-autorita-postsignum/casova-razitka

[47] Časová razítka I. – vše, co potřebujete vědět o časových razítkách. CGM svět [online]. 2019 [cit. 2023-11-28]. Dostupné z: https://blog.cgmsvet.cz/casova-razitka-i-vse-co-potrebujete-vedet-o-casovych-razitkach/?at=98f42&tt=%7Bsales%7D

[48] GRIMES, Roger A. Hacking Multifactor Authentication [online]. Wiley, 2020 [cit. 2023-09-20]. ISBN 9781119650805. Dostupné z: https://www.perlego.com/book/1881873/hacking-multifactor-authentication-pdf

[49] Single-factor, Two-factor, and Multi-factor Authentication. Ping Identity [online]. c2023 [cit. 2023-11-28]. Dostupné z: https://www.pingidentity.com/en/resources/identity-

fundamentals/authentication/single-factor-two-factor-multi-factor-authentication.html

[50] Co je umělá inteligence a jak ji využíváme? Zpravodajství [online]. 2023 [cit. 2023-11-28]. Dostupné z: https://www.europarl.europa.eu/news/cs/headlines/society/20200827STO85804/umela-inteligence-definice-a-vyuziti

[51] ZANDL, Patrick. Mýty a naděje digitálního světa: vše, co potřebujete vědět o kryptoměnách, umělé inteligenci a dalších převratných technologiích. V Brně: Jan Melvil Publishing, 2022. ISBN 978-80-7555-175-7.

[52] Artificial intelligence (AI) vs. machine learning (ML). Google Cloud [online]. [cit. 2023-11-28]. Dostupné z: https://cloud.google.com/learn/artificial-intelligence-vs-machine-learning

[53] What Is the Turing Test? Built In National [online]. 2023 [cit. 2023-11-28]. Dostupné z: https://builtin.com/artificial-intelligence/turing-test

[54] What is Machine Learning? Defination, Types, Applications, and more. Great Learning [online]. 2023 [cit. 2023-11-28]. Dostupné z: https://www.mygreatlearning.com/blog/what-is-machine-learning/ [55] Deep Learning vs. Machine Learning – What's The Difference? Levity [online]. 2023 [cit. 2023-11-28]. Dostupné z: https://levity.ai/blog/difference-machine-learning-deep-learning

[56] What is Deep Learning and How Does It Works [Explained]. Simpli learn [online]. 2023 [cit. 2023-11-28]. Dostupné z: https://www.simplilearn.com/tutorials/deep-learning-tutorial/what-is-deep-learning

[57] Natural language processing (NLP). TechTarget [online]. 2023 [cit. 2023-11-28]. Dostupné z: https://www.techtarget.com/searchenterpriseai/definition/natural-language-processing-NLP

[58] Difference between Cognitive Computing and Machine Learning. Tutorialspoint [online]. 2023 [cit. 2023-11-28]. Dostupné z: https://www.tutorialspoint.com/difference-between-cognitive-computing-and-machine-learning

[59] What is Computer Vision? The Complete Technology Guide for 2024. Viso.ai [online]. [cit. 2023-11-28]. Dostupné z: https://viso.ai/computer-vision/what-is-computer-vision/

[60] RUSSELL, Stuart J. Jako člověk: umělá inteligence a problém jejího ovládání. Populární práce. Zip., svazek 76. Praha, 2021. ISBN 978-80-7363-810-8.

[61] Chí-kvadrát test v kontingenčních tabulkách. MATH AND STATS SUPPORT CENTRE [online]. [cit. 2023-12-08]. Dostupné z: https://mathstat.econ.muni.cz/media/19046/chikv.pdf?fbclid=IwAR0lGGZcyFY7ajVjB3v-yQ7aesiFXZ2J0YhKOMlal3stDdUbs39MYWkm9iE

Přílohy

Příloha A – Dotazník

Digitální důvěra

Váš studijní program

- Bakalářský
- Magisterský/inženýrský
- Doktorský

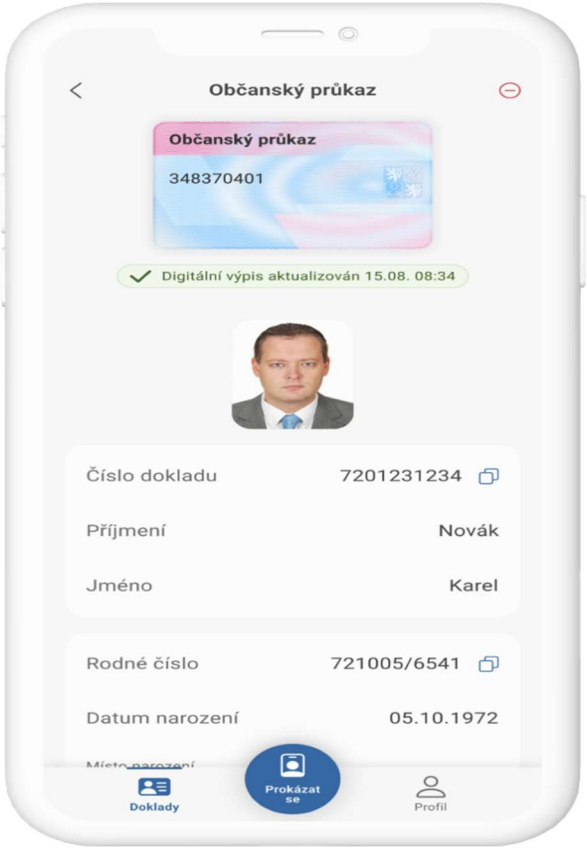
Pohlaví

- Muž
- Žena
- Jiné

1. Jak byste charakterizovali termín "digitální důvěra" a co pro vás přesně znamená?

_____

2. Slyšeli jste o mobilní aplikaci eDoklady (jedná se o aplikaci, ve které bude možné mít své identifikační doklady v digitální formě)?



- **Ano**
- **Ne**

3. Uvažujete o tom, využívat možnost prokazování se touto aplikací, až to bude možné?

- Ano
- Spíše ano
- Spíše ne
- Ne

4. Domníváte se, že je pro Vás bezpečnější mít identifikační doklad (například občanský průkaz) v podobě karty, nebo v digitální podobě v aplikaci. Jaký je váš názor na bezpečnost těchto informací?

- Více důvěřuji digitálu
- Více důvěřuji ve fyzický prvek
- Nepreferuji ani jednu z možností

5. Jak se cítíte ohledně možného zneužití osobních informací, které jste poskytli online?

- Mám silné obavy o zneužití
- Mám malé obavy o zneužití
- Nemám obavy o zneužití
- Neřeším to

6. Pokud by došlo k úniku dat z určité organizace, kde máte svůj účet a využíváte jejich služby nebo produkty, zvažovali byste, zda zůstanete jejich klientem?

- Určitě bych nezůstal nadále klientem
- Měl bych pochybnosti o setrvání klientem
- Záleží na opatřeních organizace
- Zůstal bych klientem, kdyby jejich služby a produkty nedokázal nikdo tak kvalitně zastoupit
- Zůstal bych klientem

7. Preferujete bezhotovostní platby nebo platby hotovostí při provádění nákupů?

- Pokud je to možné, tak bezhotovostní
- Spíše bezhotovostně
- Spíše hotovostně
- Hotovost

8. Jak vnímáte bezpečnost bezhotovostních plateb?

- Vysoký pocit bezpečí
- Střední pocit bezpečí

- Nízký pocit bezpečí
- Bezpečnost pro mě není prioritou

9. Použili jste někdy elektronický podpis?

- Ano, pravidelně používám elektronický podpis.
- Ano, několikrát jsem použil elektronický podpis, ale nepravidelně.
- Ne, nikdy jsem nepoužil elektronický podpis, ale jsem o něm informován/a.
- Ne, nikdy jsem nepoužil elektronický podpis a nevím, co to je.

10. Jak často zabezpečujete své účty vícefaktorovým ověřením (např. dvou faktorová autentizace – SMS kód)?

- Používám vícefaktorové ověření na všech svých účtech
- Používám vícefaktorové ověření na citlivých účtech (např. účty s penězi, citlivými informacemi, sociálními sítěmi)
- Používám vícefaktorové ověření pouze tam, kde je vyžadováno, jinak ne

11. V oblasti řešení různých záležitostí, dáváte přednost online řešením, pokud je to možné, nebo upřednostňujete osobní kontakt?

- Vždycky online řešení
- Záleží na povaze záležitosti
- Preferuji osobní kontakt
- Nemám preference

12. Získáváte častěji informace z elektronických zdrojů nebo tištěných zdrojů (knihy, časopisy atd.)?

- Výrazný podíl mají informace v elektronické podobě
- Spíše v elektronické podobě
- Rovnoměrný podíl
- Spíše informace v papírové podobě
- Výrazný podíl mají informace v papírové podobě

13. Jak moc velké obavy máte z toho, že získané informace v digitální formě mohou být falešné nebo zavádějící?

- Velmi velké obavy
- Značné obavy
- Mírné obavy
- Malé obavy
- Žádné obavy

14. Jak vnímáte trend implementace umělé inteligence do různých aspektů života (digitální asistenti (např. Siri), autonomní řízení, CHATGPT atd.)

- Velmi pozitivně
- Spíše pozitivně
- Neutrálně
- Spíše negativně
- Negativně

15. Máte obavy z využívání umělé inteligence k šíření dezinformací a fake news?

- Silné obavy
- Menší obavy
- Spíše nemám obavy
- Nemám obavy

Jako poslední otázku bych se chtěl zeptat, z jaké jste fakulty?

- Fakulta ekonomicko-správní
- Dopravní fakulta Jana Pernera
- Fakulta elektrotechniky a informatiky
- Fakulta chemicko-technologická
- Fakulta filozofická
- Fakulta restaurování
- Fakulta zdravotnických studií