ŠKODA AUTO VYSOKÁ ŠKOLA o.p.s.

Studijní program: B0413P050002 Ekonomika a management

Studijní obor/specializace: Specializace Řízení lidských zdrojů

Cyberloafing: Využívání internetu pro soukromé účely během pracovní doby

Bakalářská práce

Jarmila ŽIŽKOVÁ

Vedoucí práce: doc. PhDr. Karel Pavlica, Ph.D.

ŠKODA AUTO VYSOKÁ ŠKOLA o.p.s.
Katedra řízení lidských zdrojů

Akademický rok: 2022/2023

ŠKODA AUTO Vysoká škola

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Zpracovatelka: **Jarmila Žižková**

Studijní program: Ekonomika a management

Specializace: Řízení lidských zdrojů

Název tématu: **Cyberloafing: Využívání internetu pro soukromé účely během pracovní doby**

Cíl: Teoretickým cílem práce je podat přehled aktuálních poznatků o využívání internetu a online prostředí k plnění pracovních povinností. Praktickým cílem práce je analyzovat ve vybrané organizaci působící v oblasti bankovnictví používané formy cyberloafingu a na tomto základě navrhnout opatření zaměřená na eliminaci a prevenci využívání internetu během pracovní doby k soukromým účelům.

Rámcový obsah:

1. Úvod – vymezení a zdůvodnění cílů práce.
2. Využívání internetu a online prostředí k výkonu práce.
3. Cyberloafing.
4. Charakteristika vybrané organizace a jejích přístupů ke kontrole cyberloafingu.
5. Empirický výzkum – analýza používaných forem cyberloafingu ve vybrané organizaci.
6. Vyhodnocení výsledků empirického výzkumu a návrh opatření zaměřených na eliminaci a prevenci využívání internetu během pracovní doby k soukromým účelům.

Rozsah práce: 25 – 30 stran

Seznam odborné literatury:

1. ANANDARAJAN, M. – SIMMERS, C. *The Internet of People, Things and Services.* New York: Routledge , 2018. 285 s. ISBN 978-1-138-74232-1.
2. GIORDANO, C. – MERCADO, B. – DILCHERT , S. A meta-analytic investigation of cyberloafing. [online]. 2017. URL: https://www.emerald.com/insight/publication/issn/1362-0436.
3. KOAY, K Y. Does Cyberloafing Really Harm Employees' Work Performance?: An Overview. [online]. 2019. URL: https://www.researchgate.net/publication/325997892.
4. TAYLOR, S. – ARMSTRONG, M. *Armstrong's Handbook of Human Resource Management Practice.* Velká Británie: Kogan Page Ltd, 2020. 800 s. ISBN 978-07-494-9827-6.
5. YOGUN, A. CYBERLOAFING AND INNOVATIVE WORK BEHAVIOR AMONG BANKING SECTOR EMPLOYEES. [online]. 2015. URL: https://www.eajournals.org/wp-content/uploads/.

Datum zadání bakalářské práce: prosinec 2021

Termín odevzdání bakalářské práce: prosinec 2022

L. S.

Elektronicky schváleno dne 24. 5. 2022

Jarmila Žižková

Autorka práce

Elektronicky schváleno dne 24. 5. 2022

doc. PhDr. Karel Pavlica, Ph.D.

Vedoucí práce

Elektronicky schváleno dne 24. 5. 2022

doc. PhDr. Karel Pavlica, Ph.D.

Garant studijní specializace

Elektronicky schváleno dne 24. 5. 2022

doc. Ing. Pavel Mertlík, CSc.

Rektor ŠAVŠ

Prohlašuji, že jsem závěrečnou práci vypracoval(a) samostatně a použité zdroje uvádím v seznamu literatury. Prohlašuji, že jsem se při vypracování řídil(a) vnitřním předpisem ŠKODA AUTO VYSOKÉ ŠKOLY o.p.s. (dále jen ŠAVŠ) směrnicí Vypracování závěrečné práce.

Jsem si vědom(a), že se na tuto závěrečnou práci vztahuje zákon č. 121/2000 Sb., autorský zákon, že se jedná ve smyslu § 60 o školní dílo a že podle § 35 odst. 3 je ŠAVŠ oprávněna mou práci využít k výuce nebo k vlastní vnitřní potřebě. Souhlasím, aby moje práce byla zveřejněna podle § 47b zákona č. 111/1998 Sb., o vysokých školách.

Beru na vědomí, že ŠAVŠ má právo na uzavření licenční smlouvy k této práci za obvyklých podmínek. Užiji-li tuto práci, nebo poskytnu-li licenci k jejímu využití, mám povinnost o této skutečnosti informovat ŠAVŠ. V takovém případě má ŠAVŠ právo ode mne požadovat příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to až do jejich skutečné výše.

V Mladé Boleslavi dne 30.11.2022

Touto cestou bych v první řadě ráda poděkovala doc. PhDr. Karlu Pavlicovi, Ph.D. za odborné vedení, vstřícnost a cenné rady. Dále mockrát děkuji Ing. Michalovi Platilovi za pomoc a ochotu při zpracovávání praktické části této práce.

Obsah

Seznam použitých zkratek a symbolů

ARPA	Advanced Research Projects Agency
BYOD	Bring Your Own Device
ČSOB	Československá obchodní banka
DARPA	Defense Advanced Research Projects Agency
FNC	Federal Networking Council
VDE	Virtual Desktop Environment

Úvod

Teoretickým cílem této práce je podat přehled aktuálních poznatků o využívání internetu a online prostředí k plnění pracovních povinností. Praktickým cílem práce je analyzovat ve vybrané společnosti působící v oblasti bankovnictví, konkrétně v Československé obchodní bance, vyskytující se formy cyberloafingu a na tomto základě navrhnout opatření zaměřená na eliminaci a prevenci využívání internetu během pracovní doby k soukromým účelům.

Internetu a následně internetu v pracovním prostředí bude věnována pozornost v první kapitole této práce. Budou zde zmíněny jak jeho přínosy, tak jeho negativní vlivy v pracovním prostředí. Dále budou uvedeny základní právní aspekty užívání internetu a výpočetních technologií poskytnutých ze strany zaměstnavatele v českém právu. Závěr této kapitoly bude pojednávat o politikách lidských zdrojů.

Ve druhé kapitole bude vymezen pojem cyberloafing, dále bude představena typologie cyberloafingu. Prezentovány budou rovněž důsledky a výchozí předpoklady podílející se na výskytu cyberloafingu.

Třetí kapitola poskytne v úvodu bližší informace o Československé obchodní bance a skupině KBC. Následně budou charakterizovány přístupy organizace k cyberloafingu. Zprvu bude představen etický kodex společnosti a zásadní hodnoty a principy z něho vycházející. Pozornost bude dále v této kapitole směřována na politiky týkající se užívání internetu a komunikačních prostředků.

Detaily týkající se výzkumu, tj. výzkumná metoda a výzkumný vzorek budou popsány ve čtvrté kapitole, kde budou data získaná z výzkumu následně analyzována.

Pátá a závěrečná kapitola práce poskytne přehled výsledků výzkumu, dojde k identifikaci jednotlivých typů cyberloafingu. Na závěr budou uvedena doporučení týkající se opatření zaměřená na prevenci užívání přístupu k internetu za soukromými účely během pracovní doby. Ta budou vycházet jak ze zkoumání skutkového stavu, tak z poznatků z teoretické části práce.

Téma bylo primárně zvoleno, jelikož cyberloafing představuje rozsáhlý fenomén v pracovním prostředí, avšak v české literatuře, na rozdíl od té světové, je mu věnována minimální pozornost. Dalším důvodem výběru daného tématu bylo téměř

automatické spojení cyberloafingu a kontraproduktivního chování ve velké části zahraniční literatury. Snaha tedy směřovala také k zjištění možných pozitivních důsledků a obecně k obeznámení čtenáře s tímto v České republice ne příliš zmiňovaným tématem.

1 Využívání internetu a online prostředí k výkonu práce

Internet na pracovišti už dnes organizacím neposkytuje konkurenční výhodu, jak tomu bylo před více než dvěma desítkami let. Nyní je internet nepostradatelnou součástí firem. A ačkoliv s sebou přináší řadu výhod, existuje zde i řada úskalí, kterým je nutno v organizacích věnovat pozornost.

V první polovině této kapitoly bude pozornost věnována definici internetu a jeho vývoji v čase. Následně bude kapitola pojednávat o internetu v pracovním prostředí, jeho přínosům, rizikům spojených s jeho užíváním a právní úpravě užívání.

1.1 Internet

Internet představuje globální informační systém, prostředek pro spolupráci a interakci mezi jednotlivci a jejich počítači bez ohledu na jejich geografickou polohu. Internet byl poprvé v roce 1995 definován organizací FNC (Federal Networking Council). Dle jejich definice je internet globální informační systém, který je:

i. *„logicky propojený v globálně unikátním adresním prostoru, který je založen na internetovém protokolu (Internet Protocol – IP) či na jeho nadcházejícími rozšířeními,*
ii. *je schopný podporovat komunikaci skrze protokol Transmission Control Protocol/Internet Protocol (TCP/IP) či skrze jeho následující rozšíření nebo jiné IP kompatibilní protokoly,*
iii. *poskytuje, používá nebo umožňuje přístup, ať veřejně či privátně, k vysoce úrovňovým službám založených na této komunikaci a infrastruktuře zde popsané“* (Leiner a kol., 2009, s.30).

1.2 Vývoj internetu

Internet má svůj počátek v 50. letech minulého století ve Spojených státech amerických. Impulsem k odstartování výzkumu v počítačových a síťových komunikacích byl rok 1957, kdy tehdejší Sovětský svaz vypustil první umělou vesmírnou družici Země – Sputnik 1. Obavy z technologické nadřazenosti Ruska nad Spojenými státy americkými vedly roku 1958 k vytvoření organizace Advanced Research Projects Agency (ARPA, dneska známa pod zkratkou DARPA), financované Pentagonem. Jelikož v té době panovala Studená válka a Spojené státy se obávaly možného jaderného útoku ze strany Sovětského svazu, byl kladen

důraz na vybudování národního komunikačního systému, který by zůstal funkční v případě jaderného útoku (Bradner, 2019).

S koncepcí takového komunikačního systému přišel již v roce 1962 Paul Baran, vědecký pracovník Rand Corporation (Nondek a Řenčová, 2000). Následně byl roku 1969 představen organizací ARPA projekt ARPANET. Jednalo se o decentralizovanou síť fungující na principu přepojování paketů. Na podzim roku 1969 byl nainstalován první uzel sítě na University of California Los Angeles (UCLA) a 29. října došlo k poslání první zprávy mezi dvěma uzly – mezi UCLA a Stanford Research Institute. Do konce téhož roku byla síť rozšířena na celkový počet 4 uzlů (Leiner a kol., 2009).

Další významnou událostí v historii ARPANETu bylo v roce 1983 přijmutí standardního protokolu TCP/IP, který umožnil komunikaci mezi počítači bez ohledu na jejich operační systém. To bylo následováno rozdělením ARPANETu na vojenskou část MILNET a ARPANET, který sloužil k vědeckým účelům (Leiner a kol., 2009; Nondek a Řenčová, 2000). Roku 1990 převzal úlohu páteřní sítě NSFNET a původní ARPANET byl odstaven (Peterka, 1995).

Novou éru internetu přinesla jeho komercializace v roce 1993, kterou roku 1998 následovalo odstavení NSFNETu, jehož přenosové funkce byly převedeny do komerčního sektoru (NSF, 2003).

Česká republika byla oficiálně připojena k internetu 13. února 1992 na ČVUT v Praze (Peterka, 1995).

Během 90. let tak došlo ke změně způsobu užívání internetu, z původně armádní a výzkumné sítě, se síť postupně rozrostla do akademické, civilní a komerční sféry.

1.3 Internet v pracovním prostředí

Internet v pracovním prostředí umožňuje přístup k velkému množství informací a dle potřeby k jejich uchovávání a zpracování. Nadále usnadňuje komunikaci, ať už se jedná o interní komunikaci mezi pracovníky či odděleními v rámci jedné organizace, či externí komunikaci s klienty nebo obchodními partnery. Jednou z dalších výhod je možnost crowdsourcingu při plnění úkolů a projektů, na kterých se podílí větší počet pracovníků (White, Behrend a Siderits, 2020). Dle Anandarajana, Simmerse a Tea (2006) může užívání internetu zvýšit produktivitu.

Internet navíc společně s technologickým pokrokem vnesl do pracovního prostředí flexibilitu. Pracovníci již nejsou vázáni pouze na své pracovní místo, ale prostřednictvím přenosných zařízení jako jsou laptopy, tablety a chytré telefony a díky přístupu ke Cloudu, tak mají umožněný přístup k práci prakticky kdykoliv a odkudkoliv, pokud to povaha práce a zaměstnavatel umožňuje (Simmers a Anandarajan, 2018).

Ačkoliv spojení internetu a technologií jsou nápomocnými prostředky k usnadnění práce, tak pracovníci s přístupem k internetu představují pro organizace jisté riziko. V praxi se organizace mohou potýkat s deviantním chováním pracovníků, se ztrátou jejich produktivity či s riziky ilegálních aktivit zaměstnanců v kybernetickém prostoru, které jsou mnohdy spojeny právě s neoprávněným užíváním internetu k soukromým účelům během pracovní doby (Anandarajan, Simmers a Teo, 2006).

1.4 Právní úprava

Nejenom z výše avizovaných důvodů jsou přístup k internetu a užívání výpočetních technologií právně upraveny. Primární úpravu nalezneme v zákoně č. 262/2006 Sb., zákoník práce, v praxi se ale často setkáváme s další úpravou, a to prostřednictvím politik lidských zdrojů.

1.4.1 Zákoník práce

Zákoník práce přestavuje základní právní předpis na úseku pracovního práva, upravující především právní vztahy mezi zaměstnavateli a zaměstnanci při výkonu závislé práce nebo v souvislosti s ním (Ministerstvo práce a sociálních věcí).

Užívání výpočetní techniky upravuje konkrétně § 316 odst. 1, který zakazuje zaměstnanci bez souhlasu zaměstnavatele užívat k osobním účelům výrobní a pracovní prostředky zaměstnavatele včetně výpočetní techniky a telekomunikačního zařízení. Zaměstnavatel je dodržování tohoto zákazu oprávněn přiměřeným způsobem kontrolovat. Přiměřeným způsobem se zde rozumí například to, že při kontrole zaměstnavatel nezasahuje nad míru nezbytně nutnou do soukromí kontrolovaného zaměstnance (Tomšej, 2022). Tento paragraf lze vztáhnout i na užívání internetu, neboť jak uvádí Morávek (2017) pojem „prostředky telekomunikační či výpočetní techniky“ nelze považovat za přesný, jelikož se v praxi

ještě mimo tato zařízení jedná o služby s nimi souvisejícími, které jsou hrazeny zaměstnavatelem. Jedná se například o mobilní data, mobilní či internetový tarif.

Následující dva odstavce, tj. odst. 2 a 3 § 316 se vážou k monitoringu zaměstnanců. Dle druhého odstavce „*zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole zásilek adresovaných zaměstnanci*“ (Zákon č. 262/2006 Sb.).

V případě, že nastane závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele, který ostatně Zákoník práce blíže nespecifikuje, je zaměstnavatel dle § 316 odst. 3 oprávněn zavést kontrolní mechanismy, ale pouze za předpokladu, že o rozsahu a způsobech kontroly bude zaměstnanec informován (Zákon č. 262/2006 Sb.).

Při zavádění kontrolních mechanismů, bude třeba brát v potaz jejich kritéria jako jsou potřebnost, vhodnost, nutnost a přiměřenost. Kontrola bude možná pouze za předpokladu, že bude zvolený prostředek schopný dosáhnout sledovaného účelu, nebude zároveň existovat lepší prostředek k provedení kontroly, který by zasahoval srovnatelně nebo méně do osobnostních práv zaměstnance a zároveň bude maximálně minimalizován zásah do osobnostních práv zaměstnance. Za potřebí je taktéž dbát na skutečnost, že pokud dochází při monitoringu současně ke zpracování osobních údajů, je třeba rovněž aplikovat právní úpravu na ochranu osobních údajů, tj. nařízení Evropského parlamentu a Rady EU 2016/679 (GDPR) (Morávek, 2017).

1.4.2 Politiky lidských zdrojů

Politiky lidských zdrojů (též personální politika) definují přístupy ke klíčovým aspektům řízení lidských zdrojů v organizaci. Jsou návodem, který umožňuje řešit dílčí záležitosti týkající se řízení lidských zdrojů konzistentně dle hodnot organizace a v souladu s definovanými zásadami. Mohou existovat ve formě všeobecných prohlášení k hodnotám organizace, tj. ve formě celkové politiky anebo se mohou přímo týkat specifických oblastí. Celková politika popisuje hodnoty týkající se zacházení s lidmi, a to konkrétně z pohledu společenské odpovědnosti organizaci

vůči zaměstnancům. Specifické politiky lidských zdrojů se týkají už konkrétních oblastí jako například disciplíny, šikany, rozvoje zaměstnanců, stížností, rovných příležitostí, bezpečnosti a ochrany zdraví při práci, a právě také politiky emailů a internetu (Armstrong a Taylor, 2020).

Politika emailů a internetu v praxi nejčastěji zakazuje využívání pracovní emailové adresy pro osobní účely a vymezuje, zda zaměstnavatel poskytuje či neposkytuje souhlas k využívání internetu k soukromým účelům.

Politika lidských zdrojů je v organizacích upravována prostřednictvím vnitřních předpisů. Vnitřní předpisy můžeme definovat jako písemné normy, které blíže rozvádí pracovněprávní předpisy, zakotvení procesů a postupů v organizaci. Práva stanovená vnitřním předpisem mohou být pro zaměstnance výhodnější, než jak stanoví zákon (Tomšej, 2022).

Samotný zákoník práce stanovuje pouze dva závazné předpisy, jejichž problematika je v případě soudního sporu vymahatelná. Těmito předpisy jsou vnitřní předpis a pracovní řád. Vnitřním předpisem může zaměstnavatel stanovit práva z nichž je oprávněn zaměstnanec, běžně se jedná o mzdová nebo platová pravidla či další pracovní podmínky. Pracovní řád je zvláštním druhem vnitřního předpisu, který umožňuje zaměstnavateli detailněji rozvést či upřesnit úpravu pracovních povinností zaměstnavatele a zaměstnance. V pracovním řádu zaměstnavatel upravuje například: pracovní dobu, evidenci docházky, ohlášení a evidenci pracovních či jiných úrazů a upřesnění, v jakých případech dochází dle zaměstnavatele k porušení povinností zaměstnance, které vyplývají z právních předpisů.

Zákoník práce ukládá zaměstnavatelům stanoveným v taxativním výčtu povinnost vydání pracovního řádu. Jedná se například o Policii ČR, Bezpečnostní informační službu, Českou národní banku, krajské úřady apod. (Neščáková, 2012).

2 Cyberloafing

Jak už bylo v předchozí kapitole zmíněno, s rozšířením internetu a technologií do pracovního prostředí se rozšířila i možnost zneužívání internetu. Lim a Rajah (2018) poukazují na fakt ubývajících restrikcí týkajících se přístupu k webovým stránkám, jelikož jsou zdrojem velkého množství informací potřebných pro udržení konkurenceschopnosti organizace. Tato skutečnost vede v mnoha případech ke zvýšené míře cyberloafingu, který je definován v následující podkapitole.

2.1 Definice cyberloafingu

Cyberloafing představuje jakékoli dobrovolné užívání přístupu k internetu a emailu k čistě osobním účelům během pracovní doby (Lim, 2002). Kim a Byrne (2011) pak definují termín cyberloafing jako dobrovolné, bezcílné a neřízené užívání přístupu k internetu, které vede k nepracovním aktivitám. Ačkoliv byl cyberloafing zpočátku spjat pouze s počítačem, novější studie berou v potaz rozmach technologií a zahrnují do definice nejen zařízení jako jsou laptopy, tablety, ale i chytré telefony (Mercado, Giordano a Dilchert, 2017).

Termín cyberloafing poprvé použil Tonny Cummins v New York's Daily News v roce 1995. Do většího povědomí ho přivedla až v roce 2002 profesorka Lim svou odbornou studií, která byla publikována v Organizational Behaviour Journal (Selwyn, 2008). Termín vznikl složeninou dvou anglických slov – loafing a cyber. Slovo loafing (odvozeno od slova loafer, v překladu povaleč, mrhač času) znamenající potloukání se a slovo cyber, které bylo v roce 1995 používáno jako předpona ke slovům spjatých s počítačovou vědou (Jandaghi a kol., 2015).

V literatuře bývají kromě termínu cyberloafing používány další termíny zahrnující například:

- cyberslacking,
- online loafing,
- non-work related computing,
- problematic internet use,
- personal web usage at work,
- internet abuse (Kim a Byrne, 2011).

Zpočátku byl pojem cyberloafing v odborných studiích spojován pouze s deviantním a kontraproduktivním chováním na pracovišti (Lim, 2002; Rajah a Lim, 2018). S přibývajícím počtem studií na tuto problematiku se však začaly objevovat i takové, které poukazují na možné pozitivní účinky (Chao a kol., 2020; Blanchard a Henle, 2008).

2.2 Typologie cyberloafingu

Studie identifikují několik typů cyberloafingu. Jelikož došlo v průběhu času k řadě změnám zahrnujících například vývoj technologií nebo rozvoj sociálních sítí, existuje řada rozdílných typologií cyberloafingu.

Jednu z prvních typologií cyberloafingu představila profesorka Lim (2002), která rozdělila cyberloafing na následující dvě aktivity:

- prohlížení webů/surfování na internetu a
- emailové aktivity.

Ke kterým následně po několika letech doplnila ještě třetí aktivitu – interakce na sociálních sítích (Rajah a Lim, 2018).

Li a Chung (2006) dále rozdělili čtyři funkce internetu, prostřednictvím nichž může docházet k cyberloafingu:

- sociální funkce (např. komunikace s přáteli a kolegy),
- informační funkce (např. vyhledávání a získávání informací),
- volnočasová funkce (např. využívání internetu k zábavě),
- emoční funkce (např. gambling a seznamovací aplikace) (Yogun, 2015).

Další, které se věnovaly typologii cyberloafingu, byly Blanchard a Henle (2008). Ve své studii navázaly na poznatky Robinsona a Benetta[1] (1995) a rozlišily cyberloafing dle závažnosti:

- méně závažný cyberloafing (minor cyberloafing),
- závažný cyberloafing (serious cyberloafing).

[1] Robinson a Bennett (1995) definují deviantní chování na pracovišti jako dobrovolné chování, prostřednictvím kterého dochází k porušování zásadních norem organizace a tím současně k ohrožení blaha organizace, jejích zaměstnanců či obojího.

Ve své definici zahrnují do méně závažného cyberloafingu aktivity jako posílání a čtení osobních emailů, navštěvování webových stránek, ať už se jedná o zpravodajství, sport nebo finance. Poukazují také na fakt, že tyto aktivity jsou ve své povaze srovnatelné s tolerovanými, avšak ne příliš vhodnými aktivitami na pracovišti, kterými jsou například přijímání osobních hovorů, čtení tisku či osobní konverzace mezi kolegy. Do závažného cyberloafingu pak zahrnují aktivity jako online gambling, hraní online her a stahování hudby.

Mahatanankoon, Anandarajan a Igbaria (2004) pracují ve své studii prvotně s pěti různými aktivitami:

- nakupování a osobní podnikání,
- vyhledávání a prohlížení informací,
- interpersonální komunikace,
- zábava a trávení času,
- personální stahování souborů.

V závěru své studie však konstatují, že nejčastěji se v praxi objevují následující aktivity: nakupování a osobní podnikání, vyhledávání a prohlížení informací a interpersonální komunikace.

Z typologie Mahatanankoona, Anandarajana a Igbaria vychází Ramayah (2010) a definuje čtyři rozdílné možnosti osobního využívání internetu během pracovní doby:

- stahování souborů,
- vyhledávání informací,
- osobní komunikace,
- osobní e-komerce.

2.3 Důsledky cyberloafingu

V souvislosti s cyberloafingem existují studie zkoumající především jeho negativní důsledky. Ačkoliv je primárně vnímán jako negativní jev, je nutné kromě negativních věnovat pozornost i jeho možným pozitivním důsledkům.

2.3.1 Pozitivní důsledky cyberloafingu

Jedním z nejčastěji zkoumaných důsledků je vliv cyberloafingu na pracovní výkon. Přestože se organizace obávají akceptovat do jisté míry cyberloafing z důvodu snížení pracovního výkonu, Henle a Blanchard (2008) uvádějí, že cyberloafing může dočasně snížit stres. A za předpokladu, že cyberloafing slouží jako krátká přestávka od práce, může pozitivně přispívat ke spokojenosti zaměstnance a vést ke zlepšení pracovního výkonu (Lim a Chen, 2012). Nicméně, jak ukazuje studie Lim a Chen (2012), ne všechny aktivity mají pozitivní vliv na pracovní výkon. Například vyřizování nepracovních emailů má negativní vliv, jelikož je při této aktivitě zapotřebí vydání energie a soustředěnosti. Naopak surfování na internetu umožňuje zaměstnanci odpočinout si od práce a zmírnit stres. Jak už potvrzuje řada studií, rozhodujícím faktorem u cyberloafingu ve vztahu k pracovní výkonnosti je čas.

Krátkodobý cyberloafing podporuje navíc kreativitu a může sloužit jako prostředek osobního rozvoje a vzdělávání (Koay a Soh, 2019; Sao a kol., 2020). Jak uvádí Derin a Gökçe (2016), pozitivní vliv má rovněž na inovativní myšlení a z tohoto důvodu by organizace měly pouze definovat akceptovatelné limity cyberloafingu a nikoliv se ho snažit zcela eliminovat.

V neposlední řadě může sloužit jako prostředek k obnovení work-life-balance. Zaměstnanci mohou mít v současné době pocit, že díky technologiím neexistuje jasná hranice mezi pracovním a soukromým životem. Což způsobuje fakt, že pracovní telefon či email je dělá dostupnými prakticky na 24-hodinové bázi (Lim a Teo, 2005).

2.3.2 Negativní důsledky cyberloafingu

Jak už bylo zmíněno, negativní důsledky jsou nejčastěji spojovány se sníženým pracovním výkonem. Nejedná se však o jediný potenciální důsledek. Ačkoliv si to zaměstnanec dopouštějící se cyberloafingu nemusí uvědomovat, může organizaci vystavit hned celé řadě rizik. Tato rizika lze rozdělit do tří skupin: finanční, právní a kybernetická.

Z finančního hlediska přináší cyberloafing organizacím finanční ztráty nejčastěji z důvodu neproduktivního času stráveného v práci a následně soudních výloh. Jak

uvádí University of Nevada, americké podniky stojí roční cyberloafing více než 85 milionů dolarů (Alder, Noel a Ambrose, 2006).

Z hlediska právních záležitostí se může zaměstnanec neoprávněným stahováním souborů dopustit porušení autorského zákona, což může vyústit v právní následky jak pro zaměstnance, tak pro celou organizaci a tím tak poškodit dobrý obraz organizace v očích veřejnosti (Al-Shuaibi, Shamsudin a Subramaniam, 2013).

V poslední řadě stahováním zakázaných, nelicencovaných a neautorizovaných materiálů a navštěvováním nebezpečných webových stránek dochází k ohrožení kybernetické bezpečnosti organizace. Jelikož takovýmto počínáním zaměstnanec vystavuje organizaci hrozbám počítačových virů jako jsou například malware či ransomware (Koay a Soh, 2019).

2.4 Výchozí předpoklady podílející se na výskytu cyberloafingu

Pro správný přístup k cyberloafingu je rovněž důležité věnovat se faktorům podílejících se na jeho výskytu. Tyto předpoklady jsou nejčastěji zkoumány na třech rovinách. Jandaghi a kol. (2015) a Weissenfeld, Abramova a Krasnova (2019) dělí výchozí předpoklady na organizační, pracovní a osobní. Ozler a Polat (2012) pak přichází s individuálním, organizačním a situačním rozdělením. V této práci bude prezentováno rozdělení dle Jandaghi a kol. a Weissenfeld, Abramové a Krasnové.

2.4.1 Organizační faktory

Mezi organizační faktory ovlivňující míru cyberloafingu lze zahrnout internetovou politiku, monitoring a kontrolu zaměstnanců, sankce, organizační spravedlnost a velikost organizace.

Weissenfeld, Abramova a Krasnova (2019) ve své studii uvádí, že politika opravňující zaměstnance využívat internet i k soukromým účelům podněcuje cyberloafing. Naopak monitoring, potenciální sankce, jasná a transparentní opatření vedou ke snížení cyberloafingu (Weissenfeld, Abramova a Krasnova, 2019; Jandaghi a kol., 2015). V poslední řadě zamezuje cyberloafingu vysoká organizační spravedlnost (Lim, 2002).

2.4.2 Pracovní faktory

Pracovní faktory zahrnují pracovní požadavky, pracovní pozici, smysluplnost práce, pracovní spokojenost, stres, kreativitu práce, plat/mzdu, míru nudy a vztah k nadřízeným.

Obecně zaměstnanci pracující na vyšších pozicích s vyšším příjmem, kteří jsou vystaveni více stresu mají vyšší tendenci schylovat se k cyberloafingu. K cyberloafingu může vést i nuda či nedostatek vyžadované činnosti během pracovní doby nebo naopak úplně opačný případ, kdy jsou na zaměstnance kladeny příliš vysoké nároky (Weissenfeld, Abramova a Krasnova, 2019; Jandaghi a kol., 2015).

2.4.3 Osobní faktory

Osobními faktory jsou například osobnostní rysy, demografické faktory, vnímaná užitečnost cyberloafingu, internetové a počítačové dovednosti, vzdělání, svědomitost, sebekontrola, emoční inteligence a sklony k prokrastinaci.

Dle Phillipse (2006) se na cyberloafingu budou s větší pravděpodobností podílet extroverti, což potvrzuje i studie Lim a Chena (2012), ve které je navíc uvedeno, že jedinci s vyšším sebevědomím a nižšími stupni úzkosti se budou pravděpodobněji účastnit cyberloafingu. Lim a Chen (2012) ve své studii rovněž zkoumali rozdíl v přístupech k cyberloafingu mezi pohlavími. Následně došli k závěru, že muži se budou podílet na cyberloafingu patrně více než ženy. Tyto závěry jsou následně potvrzeny studií Weissenfeld, Abramové a Krasnové (2019), které ještě blíže specifikují, že pravděpodobnost cyberloafingu je vyšší u mladých extrovertních mužů, kteří jsou zkušenými uživateli výpočetní techniky. Nadále pokud jedinci budou považovat cyberloafing za užitečný (např. ho budou vnímat jako potřebnou přestávku od práce), budou se ho také účastnit ve vyšší míře. K cyberloafingu mezi jiné pozitivně přispívá i úroveň vzdělání. Naopak negativní vliv na cyberloafing mají svědomitost, sebekontrola a emoční inteligence.

3 Charakteristika vybrané organizace a jejích přístupů ke kontrole cyberloafingu

3.1 Představení organizace

Československá obchodní banka, a.s. (dále jen ČSOB) je univerzální bankou působící v České republice. Její vznik se datuje do roku 1964, kdy byla založena státem za účelem poskytování služeb v oblasti financování zahraničního obchodu a volnoměnových operací. I po rozdělení Československa roku 1993 pokračovaly aktivity ČSOB na českém a slovenském trhu. V červnu roku 1999 došlo k privatizaci ČSOB a jejím majoritním vlastníkem se stala belgická KBC Bank NV, 100% dceřiná společnost mezinárodní bankopojišťovací skupiny KBC Group NV. V roce 2000 ČSOB převzala Investiční a Poštovní banku (IPB). Roku 2007 došlo k odkoupení minoritních podílů bankou KBC Bank, která se tím stala jediným akcionářem ČSOB. Až do konce roku 2007 působila ČSOB na českém i slovenském trhu, k 1. lednu 2008 byla slovenská organizační složka ČSOB transformována do samostatné právnické osoby, která je ovládána společností KBC Bank prostřednictvím 100% podílu na hlasovacích právech (ČSOB).

V roce 2019 byla uzavřena dohoda o koupi zbývajícího 45% vlastnického podílu Českomoravské stavební spořitelny (ČMSS), která byla dosud vlastněna společností Bausparkasse Schwäbisch Hall. ČSOB se stala touto akvizicí jediným akcionářem ČMSS a zároveň tak posílila svoji pozici lídra trhu v oblasti financování bydlení. Následně o rok později došlo k přejmenování ČMSS na ČSOB Stavební spořitelnu (ČSOB).

ČSOB soustřeďuje svoji činnost do všech klientských segmentů, tj. od fyzických osob, přes malé a střední podniky až po korporátní a institucionální klientelu (ČSOB).

3.1.1 Skupina ČSOB

Finanční skupina ČSOB zahrnuje Banku a strategické společnosti spojené s ČSOB, které jsou buď přímo či nepřímo ovládané ČSOB, či případně KBC. Jedná se především o Hypoteční banku, ČSOB Pojišťovnu, ČSOBS, ČSOB Penzijní společnost, ČSOB Leasing, ČSOB Factoring, Patria Finance a Ušetřeno.cz.

Skupina ČSOB nabízí své klientele širokou nabídku bankovních produktů a služeb, mimo ty standardní se do jejího produktového portfolia řadí:

- hypotéky a půjčky ze stavebního spoření,
- pojistné produkty,
- penzijní fondy,
- produkty kolektivního financování a správa aktiv,
- specializované služby (např. leasing a factoring) a
- služby spojené s obchodováním s akciemi na finančních trzích.

Strategické obchodní jednotky Skupiny ČSOB se dělí do pěti následujících segmentů:

- Retailové bankovnictví,
- Vztahové bankovnictví,
- Finanční trhy,
- Financování bydlení a
- Centrála.

Celková aktiva vykázaná k 31. prosinci 2021 činila 1 805,5 mld. Kč a čistý zisk za rok 2021 představoval 16,2 mld. Kč, což řadí skupinu ČSOB mezi tři nejvýznamnější bankovní skupiny působící na českém trhu. Dle počtu klientů je pak druhou největší bankou v České republice, kdy se svými 4,225 miliony klienty následuje Českou spořitelnu.

Skupina ČSOB k 31. prosinci 2021 zaměstnávala 8 087 zaměstnanců (ČSOB).

3.1.2 KBC Group

KBC Group se sídlem v Bruselu je integrovanou bankopojišťovací skupinou. Vznikla v roce 1998 fúzí dvou belgických bank – Kredietbank a CERA Bank – a belgické pojišťovny ABB Insurance. 60 % jejích akcií je volně obchodovaných na burze Euronext v Bruselu, 40 % akcií KBC Group pak drží kmenoví akcionáři – KBC Ancora, Cera, MRBB a ostatní kmenoví akcionáři.

V současnosti se obzvlášť zaměřuje na klientelu v oblasti fyzických osob, privátního bankovnictví, malých a středních podniků a středně velkých korporací. Jejími klíčovými trhy jsou domácí Belgie a dále Česká republika, Slovensko, Maďarsko, Bulharsko a Irsko. Přítomna je také v dalších zemích světa, byť jen omezeně, kde působí jako podpora korporátních klientů z klíčových trhů. Od roku 2013 rozvrhla KBC Group své aktivity na klíčových trzích do tří obchodních divizí – Belgie, Česká republika a Mezinárodní trhy. Mezi hlavní aktivity patří půjčky, vklady, pojištění, investice, správa aktiv, platby a jiné finanční služby (KBC).

V 6-ti klíčových zemích obsluhuje 12 milionů klientů a vlastní síť přibližně 1 200 bankovních poboček. Disponuje celkovým kapitálem 23 bilionů eur a 226 biliony eur ve vkladech a dluhových cenných papírech. Zaměstnává přibližně 40 000 zaměstnanců (všechna zmíněná čísla odpovídají stavu k 31. prosinci 2021) (KBC).

3.2 Přístupy ČSOB ke kontrole cyberloafingu

Na základě zjištění je nejprve třeba zmínit, že cyberloafingu ve skupině ČSOB není věnována konkrétní pozornost, ale je upraven prostřednictvím Etického kodexu zaměstnanců skupiny ČSOB, člena skupiny KBC a na něho vázajícími se vnitropodnikovými předpisy. Další přístupy organizace mající vliv na cyberloafing zahrnují školení, workshopy a budování povědomí.

Dle poznatků z teoretické části je také nutno brát v potaz cyberloafing ve vztahu ke kybernetické bezpečnosti organizace. V souvislosti s předmětem podnikání ČSOB a v současnosti přibývajícími kybernetickými útoky na organizace je to také nedílným faktem, na který je třeba brát zřetel a bude také podrobněji rozveden v této kapitole.

3.2.1 Etický kodex zaměstnanců skupiny ČSOB, člena skupiny KBC

Problematiku cyberloafing upravuje v prvotní řadě etický kodex v rámci Ochrany majetku skupiny. Etický kodex představuje dokument popisující zásady etického chování zaměstnanců ve vztahu ke klientům, zaměstnavateli, kolegům, dodavatelům, společnosti, konkurenci a médiím. Je základní a nejdůležitější normou, od které se odvíjejí vnitropodnikové předpisy a další specializovanější kodexy konkrétních cílových skupin. Závazný je pro všechny zaměstnance skupiny ČSOB.

Než bude věnována pozornost cyberloafingu, je vhodné pro účely této práce zmínit hlavní zásady, principy a hodnoty obsažené v etickém kodexu.

Jak uvádí etický kodex, za hlavní zásady skupiny ČSOB jsou považovány kladení zájmu zákazníka na první místo, čestnost v obchodování a korektnost ve vztazích, odpovědnost a diskrétnost při jednání, respektování zákonů, vážení si kolegů, vyznávání principů PEARL a etické jednání.

K definování kultury a hodnot chování využívá skupina ČSOB společně se skupinou KBC zkratku PEARL, která zahrnuje následující principy:

- performance (výkonnost),
- empowerment (zmocňování),
- accountability (zodpovědnost),
- responsiveness (vnímavost) a
- local embeddedness (lokální ukotvení).

Princip performance (výkonnost) představuje myšlenku „co slíbíme, to dodáme". Následující princip empowerment (zmocňování) dává prostor pro odvahu dělat věci jinými způsoby, tím, že je poskytována každému jednotlivému zaměstnanci šance pro rozvoj jeho kreativity a talentu. Princip accountability (zodpovědnost) pak značí přijímání osobní odpovědnosti za vykonávanou činnost vůči klientům, kolegům, akcionářům, ale i společnosti celkově. Dále se princip responsiveness (vnímavost) zaměřuje na vnímání druhých, na proaktivní a otevřený přístup k otázkám, návrhům, příspěvkům, připomínkám a názorům, jak klientů, tak kolegů a managementu. V neposlední řadě se princip local embeddedness (lokální ukotvení) soustředí na diverzitu svých týmů a klientely na různých klíčových trzích. Diverzita je zároveň vnímána jako silná stránka organizace.

Skupina KBC navíc v nedávné době rozšířila PEARL o znaménko „+", které symbolizuje posílení celoskupinové spolupráce napříč různými zeměmi a oblastmi. V rámci celoskupinové spolupráce si klade za cíl důraz na společný vývoj, řešení, iniciativy a sdílení nápadů, tak aby do budoucna byly jednoduše aplikovatelné v rámci celé skupiny a zajistily tak silné postavení skupiny na trhu.

Firemní kulturu společně s PEARL+ definují následující 3 hodnoty:

- respect (respekt),
- responsiveness (vnímavost) a
- results driven (zaměření na výsledek).

Hodnota respekt se týká rovnocenného zacházení s lidmi, úcty k nim a vstřícného a transparentního jednání s nimi. Vnímavost pak značí schopnost naslouchat a být otevřený vůči návrhům, vlivům, žádostem nebo snah okolí. Pod zaměřením na výsledek se pak skrývá spolupráce, která je nutná k dosažení konkrétních a měřitelných cílů a zároveň také snaha o neustálé celkové zlepšování. V druhé řadě je zde zmíněna schopnost dodat v domluveném čase, kvalitě a co možná nejefektivněji, co se týče hlediska nákladů.

Nyní už bude pozornost směřována na úpravu užívání internetu a dalších komunikačních prostředků.

Užívání komunikačních prostředků a ochranu dat rozebírá Etický kodex zaměstnanců skupiny ČSOB, člena skupiny KBC v části accountability, tj. zodpovědnosti. Ze strany ČSOB jsou zaměstnancům poskytovány telekomunikační prostředky a výpočetní technika, kterou je povoleno využívat pouze v souvislosti s výkonem pracovní činnosti, pokud tedy vnitřní předpisy nestanoví jinak. Etický kodex doplňuje v tomto ohledu ještě politika „Prevence úniku dat a zásady používání komunikačních systémů“. Jelikož je užívání výpočetní techniky úzce spjato s bezpečností, je třeba neopomenout následující politiku, která seznamuje zaměstnance s ochranou dat a zásadami informační bezpečnosti – „Politika informační bezpečnosti v ČSOB“.

3.2.2 Vnitropodnikové předpisy a politiky

Kromě etického kodexu seznamuje ČSOB své zaměstnance s dalšími vnitřními předpisy, které rozvádí a doplňují jednotlivé části kodexu. Dodržování vnitřních pracovních předpisů je rovněž požadováno a jejich dodržování je průběžně kontrolováno. Na rozdíl od etického kodexu nejsou však všechny vnitropodnikové předpisy automaticky závazné pro všechny zaměstnance skupiny. Působnost jednotlivých vnitřních předpisů se může odvíjet od jednotlivých poboček a útvarů

banky. K předpisům mají zaměstnanci vždy umožněný přístup prostřednictvím intranetu, kde jsou i pravidelně obeznamováni s jejich aktualizovanými zněními.

Výše avizované politiky Prevence úniku dat a zásady používání komunikačních systémů a Politika informační bezpečnosti v ČSOB jsou závazné pro všechny osoby, kterým jsou ze strany ČSOB poskytnuty technické prostředky či přístup k datům. Politiky zavazují tedy jak interní zaměstnance, tak externí pracovníky. Nadále se politiky vztahují i na vlastní zařízení, přes které je umožněn vstup do pracovního prostředí organizace.

Politika Prevence úniku dat a zásady používání komunikačních prostředků definuje zásady v ohledu na jednotlivé oblasti. Tyto oblasti se týkají například emailové komunikace, používání internetu, mobilních telefonů a zařízení BYOD, kterému bude dále také věnována pozornost. Ačkoliv jsou zásady přizpůsobeny jednotlivým oblastem, existují základní zásady, které platí obecně nehledě na oblast. Těmito zásadami jsou využívání komunikačních prostředků výhradně k výkonu práce a v souladu s etickými hodnotami ČSOB a zachovávání bezpečnosti a důvěrnosti dat.

Co se týká oblasti internetu, jak už bylo zmíněno, je poskytován pouze pro pracovní účely. Dále je přístup v jistých oblastech omezen. Omezeny jsou webové emaily, webová úložiště a sociální média. Tato omezení se tak pro představu vztahují na LikedIn, Facebook, Instagram, Twitter či třeba na platformu Ulož.to. Obecně se jedná o platformy, kde dochází ke shromažďování a toku velkého množství osobních dat, což je považováno za rizikový faktor z hlediska bezpečnosti. V praxi představuje například profesní sociální síť LinkedIn bezpečnostní riziko, jelikož je statisticky nejčastějším prostředkem hackerských útoků na organizace, nejčastěji formou phishingu. Platforma Ulož.to je pak riziková z hlediska možného odcizení dat.

Na výše uvedené stránky a platformy může být zaměstnanci přístup povolen na základě schválení přímého nadřízeného. Musí se však jednat o situaci, kdy je přístup nezbytný pro výkon práce. Takovou situaci může představovat například oprávnění přístupu na sociální sítě, zejména LinkedIn, pro zaměstnance HR oddělení. V tomto případě musí navíc zaměstnanci postupovat v souladu s politikou Politika používání sociálních médií.

Blokování webových stránek se týká nadále stránek, které jsou nemorální či neetické povahy nebo představují bezpečnostní riziko. V souvislosti s užíváním internetu je ještě zakázáno stahování softwaru neautorizovaného organizací a materiálu chráněného autorskými právy, což platí i pro osobní potřeby.

Další oblastí, které se politika věnuje, je oblast emailové komunikace. Emailová adresa přidělená zaměstnanci ze strany ČSOB může být využívaná výhradně pro plnění pracovních úkolů, tj. k interní komunikaci, externí komunikaci s klienty, dodavateli, popřípadě státními orgány. Není tedy povoleno ji využívat pro své osobní potřeby, které mohou představovat například rozesílání nepracovních emailů. Rovněž je zakázáno přeposílání pracovních emailů na osobní emailovou adresu zaměstnance.

Politika kromě emailové komunikace neopomíjí ani další komunikační nástroje ke spolupráci, mezi které lze zařadit například Skype nebo Microsoft Teams a jiné komunikační nástroje schválené KBC. Pro pracovní komunikaci je povoleno využívat pouze tyto nástroje, není tak povoleno využívat například aplikaci WhatsApp apod. Zároveň jako v ostatních případech není dovoleno využívání těchto nástrojů k soukromé komunikaci.

ČSOB poskytuje svým zaměstnancům v rámci programu BYOD („Bring Your Own Device“) možnost užívat k pracovním účelům své soukromé zařízení. V tomto případě je pak bezpečnost zařízení zajištěna prostřednictvím vstupu do zabezpečeného pracovního prostředí. Toho může být dosaženo využitím Microsoft Intune nebo VDE (virtuální počítač) apod. Ačkoliv se tedy jedná o soukromé zařízení uplatňují se na něj v rámci pracovního prostředí shodné mechanismy jako na zařízení poskytnutá zaměstnavatelem.

Jelikož informace a data představují pro skupinu ČSOB nejcennější aktiva, je nutno je náležitě chránit. Povinností vedení ČSOB je tak zajištění informační bezpečnosti, která má za cíl ochranu aktiv před jakýmikoliv hrozbami. Té se věnuje Politika informační bezpečnosti v ČSOB, která je nadřazenou politikou k politice Prevence úniku dat a zásady používání komunikačních systémů.

Jak tedy vyplývá z předem uvedeného, politiky zamezují negativním důsledkům cyberloafingu hlavně z hlediska bezpečnostních rizik a legálních problémů, které mohou pro organizaci při nezodpovědném chování na internetu vyvstat.

3.2.3 Budování povědomí

Zaměstnanci mají povinnost absolvovat kurzy týkající se informační bezpečnosti, tyto kurzy jsou rovněž povinni periodicky opakovat. Zmíněné kurzy musí podporovat vedení společně s vedoucími zaměstnanci a zároveň musí být dbán důraz na jejich důležitost, aby bylo dosaženo jejich účinnosti.

Mimo základní školení vzdělává ČSOB své zaměstnance a buduje u nich povědomí prostřednictvím řady workshopů, článků publikovaných na intranetu či tiskových konferencí a preventivních kampaní. V oblasti užívání internetu se nejčastěji věnují tematice kybernetické bezpečnosti a bezpečného chování na internetu.

4 Empirický výzkum – analýza forem cyberloafingu vyskytujících se v organizaci

4.1 Výzkumná metoda

Pro výzkumné účely této práce byla zvolena kvantitativní metoda, jedná se konkrétně o dotazníkové šetření. Kvantitativní metoda byla vybrána na základě jejích předností, které uvádí Hendl (2005). A to zejména z důvodu možnosti efektivního testování a validizace teorií z předešlé části této práce, dále se jednalo o poskytnutí přesných a numerických dat. Za další z předností byla považována relativně malá časová náročnost dotazníku pro respondenta při jeho vyplňování a také pro sběr a následnou analýzu dat. Je však nutno podotknout, že relativně malá časová náročnost se nevztahuje na tvorbu a přípravu dotazníku.

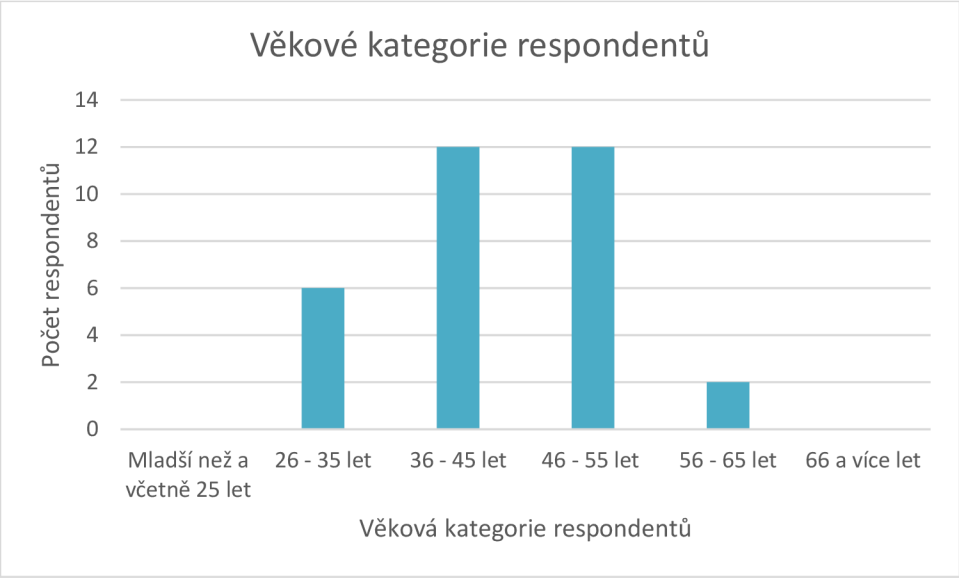
Samotný dotazník je rozdělen do tří částí, první z nich jsou demografické údaje, následující část zahrnuje zařízení, tj. výpočetní techniku a další telekomunikační zařízení a cyberloafing, poslední část dotazníku pak zkoumá politiky mající vliv na cyberloafing v organizaci. Dotazník se skládá celkem z 18 otázek, z nichž 16 je uzavřených, 1 otázka je uzavřená s volbou odpovědi „jiné“, kde respondent mohl doplnit vlastní odpověď a zbývající otázka je otevřená. Pouze u dvou otázek bylo možné zvolit více odpovědí. Stanovené otázky vycházejí ze získaných poznatků z teoretické části této práce. Přesná podoba dotazníku je uvedena v příloze v závěru práce.

Dotazník byl vytvořen v online tvůrci průzkumů Microsoft Forms. Odkaz na dotazník byl zaslán do skupinového pracovního emailu blíže neurčeného oddělení v ČSOB. To představovalo také primární důvod, proč byl zvolen právě tento nástroj, jelikož poskytoval jistotu, že daný odkaz bude na rozdíl od jiných tvůrců průzkumů funkční a nebude blokován vnitřním nastavením internetové politiky v organizaci.

4.2 Výzkumný vzorek

Výzkumný vzorek je tvořen zaměstnanci pro tuto práci blíže neurčeného oddělení organizace Československé obchodní banky, a.s. Celkem se dotazníkového šetření zúčastnilo 32 respondentů, kteří byli před vyplněním dotazníku obeznámeni s jeho přesnými účely a utvrzeni v tom, že se jedná o maximálně možně anonymní dotazník. Z tohoto důvodu není pro účely této práce tedy blíže specifikováno dané oddělení, kterého se daný výzkum týkal.

Co se týče genderového zastoupení výzkumného vzorku, jsou respondenti zastoupeni rovnoměrně. Dále byli respondenti v rámci demografických údajů rozděleni do 6 věkových kategorií. Nejpočetnějšími věkovými kategoriemi jsou kategorie 36 – 45 let a 46 – 55 let, které jsou v obou případech zastoupeny shodně 12 respondenty. Druhá nejpočetnější kategorie je 26 – 35 let s 6 respondenty, kterou následuje kategorie 56 – 65 let se 2 respondenty, přičemž věkové kategorie mladší než a včetně 25 let a 66 a více let nejsou zastoupeny vůbec. Pro přehledné znázornění je vyobrazen následující graf.



Obr. 1 Zastoupení jednotlivých věkových kategorií respondentů

4.3 Výsledky výzkumu

První dvě otázky dotazníku týkající se demografických údajů již byly vyhodnoceny v předchozí podkapitole v rámci výzkumného vzorku. Otázky následující bezprostředně po nich spadají již do sekce zařízení využívaných k cyberloafingu a vnímání cyberloafingu z pohledu zaměstnanců. Tato sekce je ještě následována třetí poslední sekcí, která věnuje svoji pozornost opatřením a politikám zavedeným v ČSOB v souvislosti s užíváním internetu.

4.3.1 Zařízení využívaná k cyberloafingu a vnímání cyberloafingu mezi zaměstnanci

Tato sekce, jak už název napovídá, se věnuje výpočetní technice a dalším zařízením využívaným během pracovní doby k pracovní činnosti a zároveň

prostřednictvím nichž se zaměstnanci mohou podílet na cyberloafingu. Následně je v této sekci zkoumán přístup a pohled na cyberloafing v řadách zaměstnanců.

Respondenti byli v první řadě dotázáni, jaký počítač využívají pro účely výkonu práce. Tato otázka byla položena, jelikož jak už bylo předem zmíněno, ČSOB poskytuje svým zaměstnancům možnost používat své soukromé zařízení k výkonu práce v rámci programu BYOD. Dále byla tato otázka zvolena z důvodu, poněvadž se na základě zjištění z teoretické části předpokládalo, že právě počítač poskytnutý zaměstnavatelem bude nejčastějším prostředkem, prostřednictvím jehož dochází k cyberloafingu. Na tuto otázku odpověděli respondenti jednomyslně a uvedli, že ke své práci využívají počítač poskytnutý zaměstnavatelem.

Následující otázka se týkala přímo cyberloafingu, kde byli respondenti tázáni, zda využívají během pracovní doby zařízení umožňující přístup na internet také k soukromým účelům. 25 respondentů odpovědělo na tuto otázku kladně. Pro respondenty, kteří přiznali využívání internetu během pracovních hodin také pro své soukromé účely, byla určena navazující otázka, která zjišťovala, jaká zařízení pro tento typ využití používají. Jednalo se o otázku s možností výběru více odpovědí. Četnost výskytu jednotlivých odpovědí je zmapována v následující tabulce.

Tab. 1 Četnost odpovědí k otázce: „Jaké zařízení používáte k soukromým účelům během pracovní doby?“

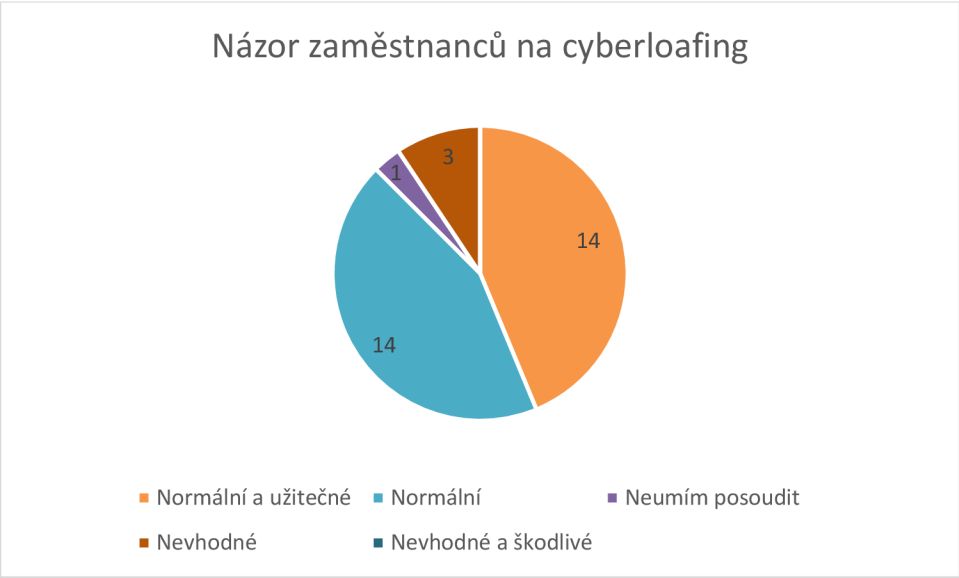
Odpověď	Četnost odpovědí
Počítač (stolní počítač, notebook, laptop apod.) poskytnutý zaměstnavatelem	22
Tablet poskytnutý zaměstnavatelem	0
Mobilní telefon poskytnutý zaměstnavatelem	3
Soukromý počítač	7
Soukromý tablet	4
Soukromý mobilní telefon	19

Jako nejhojněji využívané zařízení k soukromým účelům během pracovní doby byl uveden počítač poskytnutý zaměstnavatelem, pro který hlasovalo 22 respondentů. Druhým nejčastěji používaným zařízením byl soukromý mobilní telefon, který uvedlo jako svoji odpověď 19 respondentů. S výrazným odstupem následoval soukromý počítač se sedmi hlasy, soukromý tablet se čtyřmi hlasy a v polední řadě mobilní telefon poskytnutý zaměstnavatelem, který byl zvolen třemi respondenty. Tablet

poskytnutý zaměstnavatelem nebyl zvolen žádným z respondentů. Jak vychází z výše uvedené tabulky, je očividné, že z hlediska četnosti však celkově dominuje využití soukromých zařízení.

Další otázka v pořadí se nadále týkala zařízení, pro účely této otázky byl vybrán pouze soukromý mobilní telefon a byl přidán ještě další parametr, a to parametr mobilních dat. Přesné znění otázky bylo následující: „Připojujete se během pracovní doby k internetu za soukromými účely z vašeho soukromého mobilního zařízení a prostřednictvím vašich mobilních dat?“. 27 z celkově dotázaných respondentů na tuto otázku odpovědělo kladně. Položením této otázky šlo principiálně o eliminování pravděpodobnosti, že zařízení bude během pracovní doby připojeno k internetu přes interní síť wifi, tj. o potvrzení, že zařízení stojí zcela mimo systém digitální kontroly organizace. Důraz byl kladen na mobilní telefon také z toho důvodu, že mnoho předešlých studií pracovalo nejčastěji s variantou, kde docházelo k cyberloafingu prostřednictvím počítače. Což bylo primárně způsobeno otázkou doby, kdy výzkumy probíhaly. Technologie, konkrétně užívání chytrých mobilních telefonů nebylo tolik rozsáhlé anebo v druhé řadě šlo čistě o opomíjení užívání chytrých mobilních telefonů obecně.

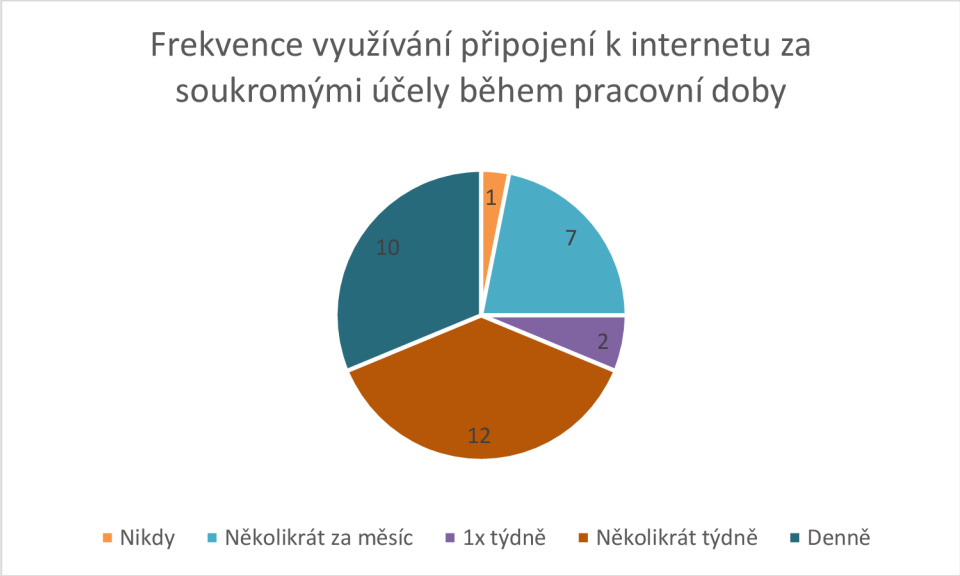
V další řadě byl zkoumán obecný názor respondentů na cyberloafing. Ti byli tázáni, zda považují používání internetu k soukromým účelům během pracovní doby za normální a užitečné, normální, nevhodné nebo za nevhodné a škodlivé. Jako další možnost odpovědi tu byla uvedena ještě možnost „neumím posoudit“. Mezi respondenty výrazně převažoval názor, že se užívání internetu k soukromým účelům během pracovní doby nijak nevymyká normalitě. 14 dotázaných k němu sdílí pozitivní postoj, jelikož ho považují za normální a užitečné, dalších 14 dotázaných to považuje za normální. Pouze 3 respondenti považují toto jednání za nevhodné. Zbývající respondent uvedl, že to neumí posoudit. Četnost odpovědí je graficky znázorněna v následujícím obrázku.



Obr. 2 Názor zaměstnanců na cyberloafing

V rámci cyberloafingu bylo nadále zjišťováno, zda-li představuje povolení od zaměstnavatele používat internet k soukromým účelům během pracovní doby důležitý motivační faktor v případě hledání nového zaměstnání. Na základě získaných odpovědí, kdy 24 respondentů považovalo povolení využívat internet k osobním účelům jako nerelevantní faktor, ho tedy nelze pokládat za důležitý.

Následující otázka zkoumala frekvenci využívání internetu k soukromým účelům během pracovní doby. Ta byla rozdělena do pěti skupin: nikdy, několikrát za měsíc, 1x týdně, několikrát týdně a denně. Nejčastěji zvolenou možností byla možnost několikrát týdně, kterou zvolilo 12 respondentů. 10 dotázaných uvedlo, že internet navštěvují v pracovní době za soukromými účely denně. 7 respondentů se pak připojuje za těmito účely několikrát za měsíc, dva pak jednou týdně a nikdy jeden dotázaný. U možnosti „nikdy“ došlo v počtu zvolených odpovědí k nesouladu s již předem položenou otázkou „Používáte během pracovní doby zařízení umožňující přístup na internet také k soukromým účelům?“. U této předešlé otázky uvedlo 7 respondentů, že během pracovní doby připojení k internetu jinak, než k pracovním činnostem nevyužívají. Na základě zjištěných faktů, lze tedy předpokládat, že původně do své odpovědi nezahrnovali výjimečné případy, kdy internet soukromě využili. Kdežto u této otázky své výpovědi upravili a zahrnuli tyto výjimečné případy s největší pravděpodobností do možnosti „několikrát za měsíc“. Následující obrázek poskytuje grafické znázornění daných odpovědí.



Obr. 3 Frekvence využívání připojení k internetu za soukromými účely během pracovní doby

Dotazník nadále zkoumal aktivity, kterých se zaměstnanci účastní v rámci využívání internetu k osobním účelům během jejich pracovní doby. Respondenti byli požádáni, aby označili všechny aktivity, kterých se účastní. Pro případ, že by byla nějaká aktivita při tvorbě dotazníku opomenuta, popřípadě by se respondent nemohl rozhodnout, do jaké kategorie jím vykonávaná aktivita patří, byla přidána možnost „jiné“, která byla zároveň otevřenou odpovědí a respondent mohl tak tuto aktivitu blíže specifikovat. Jako nejčastější aktivita je uvedeno navštěvování zpravodajských webů, pro které hlasovalo 28 respondentů. S jistým odstupem ho následují vzdělávací účely (19 respondentů), přihlašování do osobního online bankovnictví (17 respondentů) a online nakupování, pro které se rozhodlo 12 dotázaných. Sociálně orientovaných činností, tj. sociálních sítí a sociální interakce se účastní v obou případech shodně 3 respondenti. 5 respondentů, kteří hlasovali pro pole „jiné“ navíc uvedli tyto odpovědi: navštěvování stránek IDOS a Českých drah, využití internetu k zobrazení map a vyhledávání tras a v poslední řadě k přehrávání relaxační hudby. Jeden z respondentů rovněž upřesnil, že k navštěvování zpravodajských webů využívá počítač poskytnutý zaměstnavatelem, avšak k online nakupování využívá svůj soukromý mobilní telefon. Četnost jednotlivých odpovědí mapuje následující tabulka.

Tab. 2 K otázce: „Za jakým účelem využíváte přístup k internetu k soukromým účelům během pracovní doby?“

Odpověď	Četnost odpovědí
Ke vzdělávacím účelům	19
Navštěvování zpravodajských webů	28
Sociální sítě	3
Sociální interakce	3
Online nakupování	12
Online bankovnictví	17
Hraní her	0
Stahování souborů	0
Přístup k soukromým účelům nevyužívám	1
Jiné	5

Na základě tvrzení Lim a Chen (2012) bylo rovněž zkoumáno, zda zaměstnanci skutečně vnímají cyberloafing jako prostředek k relaxaci a pauze od práce. Na otázku „Využíváte přístup k internetu k soukromým účelům za účelem odpočinku od práce?“ odpovědělo 19 dotázaných kladně.

Poslední otázka této sekce se věnovala vnímání kybernetické bezpečnosti, její přesné znění bylo: „Myslíte si, že používání internetu k soukromým účelům představuje pro Vaši organizaci riziko z hlediska kybernetické bezpečnosti?“. Odpovědi na toto téma byly různorodé. Pro 7 respondentů tento fakt představuje bezpečnostní riziko, další 4 respondenti odpověděli „spíše ano“. 9 respondentů to potom za riziko nepovažuje a 8 na otázku odpovědělo „spíše ne“. Zbývající 4 respondenti uvedli, že neví.

4.3.2 Politiky upravující přístup k internetu a užívání výpočetní techniky

Poslední sekce dotazníku věnovala pozornost politikám týkajících se užívání internetu v organizaci. Úvodní otázka zkoumala, zda se zaměstnanci zúčastnili školení, které zahrnovalo informace o pravidlech užívání internetu v jejich organizaci. 29 respondentů uvedlo, že ano. Pouze 3 uvedli, že si nevzpomínají, zda se takového školení zúčastnili.

V rámci politik byla zjišťována nadále jejich jasnost a srozumitelnost, jelikož i ta může mít zásadní vliv na výskyt cyberloafingu. Srozumitelnost a jasnost byla celkově hodnocena kladně. Pro 21 respondentů jsou opatření srozumitelná a jasná,

10 respondentů uvedlo, že opatření jsou spíše srozumitelná a jasná, kdežto pouze jeden z respondentů konstatoval, že opatření mu jasná spíše nejsou.

V této souvislosti byla zkoumána i spokojenost zaměstnanců se zavedenou politikou. I zde převažoval pozitivní postoj zaměstnanců. 25 dotázaných odpovědělo, že jim nastavení politiky vyhovuje a 3 další považují politiku za naprosto vyhovující. Naopak pouze 3 zaměstnanci uvedli politiku jako nevyhovující a zbývající respondent nedokázal posoudit, zda mu politika vyhovuje či ne. Pro variantu „naprosto nevyhovuje“ se nerozhodl niko z dotázaných.

Následující otázka vycházela z té předešlé a dále rozebírala spokojenost zaměstnanců s politikou. Konkrétně byla směřována na respondenty, kteří v poslední otázce zvolili možnost odpovědi „nevyhovuje“ nebo „naprosto nevyhovuje“ a snažila se zjistit, v čem je pro ně politika nevyhovující. Jeden z respondentů uvedl, že mu nevyhovuje blokování soukromých e-mailových schránek, osobního bankovnictví a dalších webů „bezpečného charakteru“ na počítači poskytnutým zaměstnavatelem. Dále namítal, že v předešlé finanční instituci, kde byl zaměstnán, byly všechny výše zmíněné weby a domény volně přístupné. Na závěr však doplnil, že si není vědom, zda byly v této souvislosti řešeny větší bezpečnostní incidenty. Další z respondentů považuje politiku za nevyhovující z důvodu nemožnosti poslouchání streamované hudby. Politika je také považována za nevyhovující z důvodu její přílišné rigidity.

Poslední dvě otázky věnované této sekci a zároveň celého dotazníku se zaměřovaly na konkrétní bezpečnostní opatření. Prvním z nich byl monitoring. V souvislosti s ním byli respondenti dotázáni, zda je z jejich pohledu považován za potřebný kontrolní mechanismus ve vztahu s využíváním internetu. Tento kontrolní mechanismus považuje za potřebný 24 respondentů.

Druhou a závěrečnou otázkou týkající se opatření, byla otázka, zda-li považují zaměstnanci blokování webových stránek a domén za nutný bezpečnostní prvek. Na ni respondenti odpověděli téměř jednohlasně – 31 z nich ho považuje za potřebný.

5 Závěry a formulace doporučení opatření zaměřených na prevenci využívání internetu k soukromým účelům během pracovní doby

Poslední část této bakalářské práce podává ucelený přehled o nejzásadnějších zjištěních vyplývajících z empirického výzkumu provedeného formou dotazníkového šetření mezi zaměstnanci blíže nespecifikovaného oddělení v Československé obchodní bance. Stěžejním cílem tohoto výzkumu bylo zjistit, jaké formy cyberloafingu se v dané organizaci vyskytují a na základě těchto zjištění a předchozím zmapování již praktikovaných politik, navrhnout doporučení pro možné vylepšení stávajících opatření.

5.1 Závěry výzkumu

Na základě analýzy odpovědí získaných z dotazníkového šetření lze konstatovat, že cyberloafing je obecně rozsáhlým fenoménem. Více než tři čtvrtiny zaměstnanců účastnících se šetření přiznaly, že přístup k internetu používají během pracovní doby také ke svým soukromým účelům. Jelikož dle existujících definic cyberloafingu není výhradně řečeno, zda dochází k cyberloafingu pouze prostřednictvím zařízení poskytnutého zaměstnavatelem nebo k němu může docházet i skrze soukromé zařízení, je v této bakalářské práci považováno za cyberloafing jakékoliv využívání přístupu k internetu během pracovní doby vedoucí k nepracovním aktivitám. Na základě tohoto faktu byla položena následující otázka tázající se respondentů, zda během pracovní doby používají svá soukromá zařízení a svá soukromá mobilní data k přístupu na internet. Zde došlo ještě k navýšení kladných odpovědí.

Hlavním cílem práce bylo identifikovat vyskytující se typy cyberloafingu v organizaci. Zjištěné typy cyberloafingu jsou vyhodnoceny dle typologie uvedené v teoretické části této práce. Obecně lze konstatovat, že výrazně převládala forma nesociálně orientovaného cyberloafingu. Nejčastěji zmiňovanými aktivitami bylo navštěvování zpravodajských webů, využívání přístupu internetu ke vzdělávacím účelům, přístup do osobního online bankovnictví a v poslední řadě online nakupování.

Na základě aktivit zmíněných v dotazníku je možné tyto činnosti zařadit dle typologie Rajah a Lim (2018) do kategorií prohlížení webů/surfování na internetu a ve výrazně menší míře je pak zastoupena ještě kategorie interakce na sociálních

sítích. Podle kategorizace Li a Chung (2006) je zastoupena informační a sociální funkce. Na základě typologie Mahatanankoona, Anandarajana a Igbarii (2004) se vyskytují následující kategorie: vyhledávání a prohlížení informací, interpersonální komunikace, nakupování a online podnikání. Ti také ve své studii uvádí, že tyto tři kategorie jsou v praxi nejčastěji zastoupenými, což bylo tímto výzkumem rovněž potvrzeno. Dle Ramayaha (2010) lze dané činnosti rozdělit do kategorie vyhledávání informací, osobní komunikace a osobní e-komerce. V poslední řadě byl na základě dat získaných z dotazníku identifikován dle kategorizace Blanchard a Henle (2008) méně závažný cyberloafing. V této souvislosti je ještě nutno zmínit, že všechny aktivity vybrané respondenty spadaly do této kategorie a nebyla identifikována žádná činnost vykonávaná zaměstnanci, která by spadala do závažného cyberloafingu.

V návaznosti na poznatky z teoretické části došlo k potvrzení a vyvrácení následujících tvrzení. Byla potvrzena hypotéza, že pokud zaměstnanci považují cyberloafing za normální či užitečný, účastní se ho ve vyšší míře. Naopak se nepotvrdilo tvrzení, podle kterého vedou jasná a transparentní opatření ke snížení míry cyberloafingu, poněvadž 31 z respondentů vypovědělo, že politiku týkající se užívání internetu považují za srozumitelnou a jasnou nebo spíše srozumitelnou a jasnou.

5.2 Doporučení pro opatření týkající se využívání internetu k soukromým účelům v pracovní době

V první řadě je nutno zmínit pozitivní hodnocení srozumitelnosti a jasnosti daných politik zavedených v organizaci ze strany zaměstnanců. V neposlední řadě lze také v souvislosti s opatřeními pozitivně hodnotit budování povědomí o dané problematice, zde konkrétně o bezpečnostních rizicích spojených s užíváním internetu, prostřednictvím konferencí, preventivních kampaní, či článků publikovaných na intranetu.

Co se týče využívání internetu pro soukromé účely během pracovní doby, převažuje u zaměstnanců obecně pozitivní vnímání. Dle zjištění z dotazníku lze také předpokládat, že cyberloafing může sloužit ke zvýšení spokojenosti a výkonu zaměstnanců, poněvadž je 19 respondenty považován za prostředek k relaxaci a

pauze od práce. Na základě toho je doporučeno brát v potaz i pozitivní důsledky cyberloafingu na zaměstnance ze strany organizace.

Navíc respondenti v značné míře případů uvádí jako důvod využívání přístupu na internet získávání informací, konkrétně informací o aktuálním dění a vzdělávací účely. Jedná se tedy o aktivity, které vedou k osobnímu rozvoji. Na základě tohoto lze formulovat doporučení, které se týká informovanosti zaměstnanců o možnosti navrhování témat školení přímo v rámci ČSOB.

Další z doporučení se týká soukromých zařízení. Užívání soukromých zařízení, které nejsou využívány k pracovní činnosti, sice nepředstavují pro organizaci riziko z hlediska kybernetické bezpečnosti, ale mohou představovat problém z hlediska neproduktivního času zaměstnanců a jeho nemožné digitální kontrole ze strany organizace. V případě podezření při nízké výkonnosti zaměstnance by měl být kontrolován i tento fakt, a ne pouze aktivita na pracovním zařízení, jelikož jsou soukromá zařízení k cyberloafingu četněji používaná než ta pracovní.

Ačkoliv je v cíli práce stanoveno navrhnutí opatření k eliminaci či snížení cyberloafingu, na základě zjištění z této práce by neměl být cyberloafing eliminován zcela, jelikož to může vést k negativnímu vlivu na zaměstnance, ať už je to kvůli pocitu nedůvěry ze strany zaměstnavatele či chybějícímu odreagování od práce. Navrženým doporučením je tedy do jisté míry tolerování cyberloafingu, pokud dochází k řádnému plnění pracovních povinností zaměstnanců a zaměstnanec nepředstavuje svým chováním na internetu bezpečnostní riziko pro organizaci. Je třeba zároveň brát v potaz, že jednou z hlavních rolí zde vždy hraje faktor času, který zaměstnanec cyberloafingem tráví. Ze strany organizace by také měly být vždy rozlišovány aktivity, kterých se zaměstnanci při cyberloafingu účastní. Zároveň lze konstatovat, že jako nejefektivnější opatření proti cyberloafingu se jeví blokace webových stránek a domén nepotřebných k výkonu práce.

Závěr

Hlavním a stěžejním cílem práce bylo zjistit, jaké formy cyberloafingu se vyskytují v řadách zaměstnanců v Československé obchodní bance. Za účely dosažení tohoto stanoveného cíle byl zaměstnancům na blíže neurčeném oddělení zaslán odkaz na dotazník prostřednictvím pracovního emailu. Jelikož se v určitých otázkách a ohledech jednalo o citlivé údaje, byla zaměstnancům zaručena maximálně možná anonymita. Tudíž nebylo pro účely této práce blíže specifikováno dané oddělení, na kterém výzkum proběhl. Zároveň bylo opatření zachování celkové anonymity považováno za přínosné vzhledem k výpovědní hodnotě odpovědí, neboť bylo předpokládáno, že respondenti budou v tomto případě odpovídat v souladu se skutečným stavem.

První část bakalářské práce vymezuje využívání internetu a online prostředí k výkonu práce. Zabývá se tedy v první řadě definicí internetu a jeho vývojem v čase. Následně je pozornost přesunuta k internetu v pracovním prostředí, kde se nejprve práce soustředí na výhody, ale i nevýhody, které technologický pokrok do tohoto prostředí vnesl. V této souvislosti se práce dále soustředí na právní úpravu užívání internetu a výpočetních technologií v zaměstnání v české legislativě, na kterou pak v další podkapitole navazují politiky lidských zdrojů. Vymezeny jsou specifické politiky týkající se problematiky této práce, dále jsou definovány předpisy, na základě, kterých může být politika v organizaci upravena. Jedná se konkrétně o vnitřní předpis a pracovní řád.

Bakalářská práce se věnuje cyberloafingu a z tohoto důvodu bylo tedy nutné daný pojem vymezit. Úvod druhé části práce se věnuje definici cyberloafingu, na který navazuje podkapitola zabývající se jeho typologií vycházející z řady světových studií na toto téma. V následující podkapitole je věnován prostor důsledkům cyberloafingu, a to jak těm pozitivním, tak těm negativním. V závěru této části jsou představeny výchozí předpoklady podílející se na výskytu cyberloafingu, které jsou v následujících podkapitolách dle jejich rozdělení – organizační, pracovní a osobní faktory – prezentovány.

Třetí část práce pak představuje Československou obchodní banku. Stručně popisuje její historii a produktové portfolio. Dále se zaměřuje na přístupy ČSOB ke kontrole cyberloafingu. Na úvod jsou popsány hlavní hodnoty a principy ČSOB

obsažené v Etickém kodexu zaměstnanců skupiny ČSOB, člena skupiny KBC. Pozornost je následně v další podkapitole zaměřena na specifické politiky vztahující se na užívání internetu a výpočetní techniky. Konkrétně se jedná o politiky Prevence úniku dat a zásady používání komunikačních systémů a Politika informační bezpečnosti v ČSOB.

Ve čtvrté části dochází k představení výzkumné metody a výzkumného vzorku. Následuje analýza výsledků výzkumu. V případě potřeby jsou otázky doplněny o zdůvodnění, proč byla daná otázka zahrnuta do dotazníku. Tyto důvody vycházejí nejčastěji z teoretických poznatků, popřípadě vycházejí ze zavedených politik v rámci ČSOB. V této části získá čtenář nejpodrobnější informace týkající se výzkumu.

Pátá závěrečná část poskytuje stručný přehled výsledků výzkumu, identifikuje jednotlivé typy cyberloafingu vyskytující se v ČSOB dle různých typologií uvedených v teoretické části. Zároveň vyvrací či potvrzuje tvrzení z předešlých studií. Na závěr jsou uvedena doporučení týkající se opatření užívání internetu a výpočetní techniky.

Stručná zjištění, která výzkum přinesl jsou následující:

- Identifikované typy cyberloafingu se převážně týkaly vyhledávání a prohlížení informací, interpersonální komunikace a osobní e-komerce.
- Všechny aktivity vykonávané v rámci cyberloafingu spadaly do méně závažného cyberloafingu.
- Na základě identifikovaných aktivit a s nimi souvisejícími pozitivními důsledky, je doporučeno cyberloafing do jisté míry tolerovat, pokud to nemá zásadní vliv na plnění pracovních povinností a informační bezpečnost.
- V rámci navržení opatření je doporučeno přistupovat k těmto opatřením i s ohledem na chování zaměstnanců, pokud je to možné.

Seznam literatury

ALDER, G. Stoney, Terry W. NOEL a Maureen L. AMBROSE. Clarifying the effects of Internet monitoring on job attitudes: The mediating role of employee trust. *Information & Management* [online]. 2006, **43**(7), 894-903 [cit. 2022-09-27]. ISSN 03787206. Dostupné z: doi:10.1016/j.im.2006.08.008

AL-SHUAIBI, Ahmad Said Ibrahim, Faridahwati SHAMSUDIN a Chandrakantan SUBRAMANIAM. Do human resource management practices matter in reducing cyberloafing at work: Evidence from Jordan. *Journal of WEI Business and Economics*. 2013, **2**(2).

ANANDARAJAN, Murugan, Claire A. SIMMERS a Thompson S. H. TEO. *The internet and workplace transformation*. New York: Routledge, 2006. ISBN: 0-7656-1445-6.

ARMSTRONG, Michael a Stephen TAYLOR. *Armstrong's handbook of human resource management practice*. 15th edition. New York, NY: KoganPage, 2020. ISBN 9780749498283.

BLANCHARD, Anita L. a Christine A. HENLE. Correlates of different forms of cyberloafing: The role of norms and external locus of control. *Computers in Human Behavior* [online]. 2008, **24**(3), 1067-1084 [cit. 2022-10-02]. ISSN 07475632. Dostupné z: doi:10.1016/j.chb.2007.03.008.

BRADNER, Scott. A history of the Internet [přednáška]. In: *Berkman Klein Luncheon Series* [online]. Berkman Klein Center. Published on February 5, 2019 [vid. 2022-09-06]. Dostupné z: https://cyber.harvard.edu/events/history-internet.

ČSOB. *Československá obchodní banka* [online]. 2022. [vid. 2022-11-1]. Dostupné z: https://www.csob.cz/.

ČSOB. Etický kodex zaměstnanců skupiny ČSOB, člena skupiny KBC. In: *Csob.cz* [online]. 2022. Československá obchodní banka. [vid. 2022-11-1]. Dostupné z: https://www.csob.cz/portal/documents/10710/594543/csob-csr-eticky-kodex.pdf.

ČSOB. Výroční zpráva 2021. In: *Csob.cz* [online]. 2022. Československá obchodní banka. [vid. 2022-11-1]. Dostupné z: https: //www.csob.cz/portal/documents/10710/444804/vz-csob-2021.pdf.

DERIN, Neslihan a Sinem Güravşar GÖKÇE. Are Cyberloafers Also Innovators?: A Study on the Relationship between Cyberloafing and Innovative Work Behavior. *Procedia - Social and Behavioral Sciences* [online]. 2016, **235**, 694-700 [cit. 2022-10-03]. ISSN 18770428. Dostupné z: doi:10.1016/j.sbspro.2016.11.070

HENDL, Jan. Kvalitativní výzkum: základní metody a aplikace. Praha: Portál, 2005. ISBN 80-7367-040-2.

JANDAGHI, Gholamreza, Seyed Mehdi ALVANI, Hassan Zarei MARTIN a Samira Fakheri KOZEKANAN. Cyberloafing management in organizations. *Iranian Journal of Management Studies*. 2015, **8**(3), 335-349. ISSN: 2345-3745.

KBC. Annual Report KBC Group 2021. In: *Kbc.com* [online]. 2022. KBC. [vid. 2022-11-1]. Dostupné z: https://www.kbc.com/content/dam/kbccom/doc/investor-relations/Results/jvs-2021/jvs-2021-grp-en.pdf.

KIM, Sunny Jung a Sahara BYRNE. Conceptualizing personal web usage in work contexts: A preliminary framework. *Computers in Human Behavior* [online]. 2011, **27**(6), 2271-2283 [cit. 2022-10-02]. ISSN 07475632. Dostupné z: doi:10.1016/j.chb.2011.07.006.

KOAY, Kian-Yeik a Patrick Chin-Hooi SOH. Does Cyberloafing Really Harm Employees' Work Performance?: An Overview. In: XU, Jiuping, Fang Lee COOKE, Mitsuo GEN a Syed Ejaz AHMED, ed. *Proceedings of the Twelfth International Conference on Management Science and Engineering Management* [online]. Cham: Springer International Publishing, 2019, 2019-06-26, s. 901-912 [cit. 2022-10-01]. Lecture Notes on Multidisciplinary Industrial Engineering. ISBN 978-3-319-93350-4. Dostupné z: doi:10.1007/978-3-319-93351-1.

LEINER, Barry M., Vinton G. CERF, David D. Clark, Robert E. KAHN, Leonard KLEINROCK, Daniel C. LYNCH, Jon POSTEL, Larry G. ROBERTS a Stephen WOLFF. A brief history of the internet. *ACM SIGCOMM Computer Communication Review*. 2009, 39(5), 22-31.

LI, Shih-Ming a Teng-Ming CHUNG. Internet function and Internet addictive behavior. *Computers in Human Behavior* [online]. 2006, **22**(6), 1067-1071 [cit. 2022-10-04]. ISSN 07475632. Dostupné z: doi:10.1016/j.chb.2004.03.030.

LIM, Vivien K.G. a Thompson S.H. TEO. Prevalence, perceived seriousness, justification and regulation of cyberloafing in Singapore. *Information & Management* [online]. 2005, **42**(8), 1081-1093 [cit. 2022-10-03]. ISSN 03787206. Dostupné z: doi:10.1016/j.im.2004.12.002.

LIM, Vivien K.G. a Don J.Q. CHEN. Cyberloafing at the workplace: gain or drain on work?. *Behaviour & Information Technology* [online]. 2012, **31**(4), 343-353 [cit. 2022-10-02]. ISSN 0144-929X. Dostupné z: doi:10.1080/01449290903353054.

MAHATANANKOON, Pruthikrai, Murugan ANANDARAJAN a Magid IGBARIA. Development of a measure of personal web usage in the workplace. *Cyberpsychology and Behaviour*. 2004, **7**(1), 93-104. Dostupné z: doi:10.1089/109493104322820165.

MERCADO, Brittany K., Casey GIORDANO a Stephan DILCHERT. A meta-analytic investigation of cyberloafing. *Career Development International* [online].

2017, **22**(5), 546-564 [cit. 2022-10-02]. ISSN 1362-0436. Dostupné z: doi:10.1108/CDI-08-2017-0142.

MORÁVEK, Jakub. Kontrola a sledování zaměstnanců – výklad § 316 ZPr. *Právní rozhledy*. 2017, **25**(17), 573-581.

NEŠČÁKOVÁ, Libuše. *Pracovní právo pro neprávníky: rozbory vybraných ustanovení, praktická aplikace, vzory a příklady*. Praha: Grada, 2012. Právo pro každého (Grada). ISBN 978-80-247-4091-1.

NONDEK, Lubomír a Lenka ŘENČOVÁ. *Internet a jeho komerční využití*. Praha: Grada, 2000. Manažer. ISBN 80-7169-933-0.

NSF. A brief history od NSF and the Internet. In: *National Science Foundation* [online]. 2003-08-13 [vid. 2022-09-08]. Dostupné z: https://www.nsf.gov/news/news_summ.jsp?cntn_id=103050.

OZLER, Derya Ergun a Gulcin POLAT. Cyberloafing phenomenon in organizations: Determinants and impacts. *International Journal of eBusiness and eGovernment Studies*. 2012, **4**(2). ISSN: 2146-0744.

PETERKA, Jiří. Internet u nás. In: *Archiv článků a přednášek Jiřího Peterky* [online]. 1995 [vid. 2022-09-07]. Dostupné z: https://www.earchiv.cz/a95/a504c504.php3.

PETERKA, Jiří. Na počátku byl ARPANET. In: *Archiv článků a přednášek Jiřího Peterky* [online]. 1995 [vid. 2022-09-07]. Dostupné z: https://www.earchiv.cz/a95/a504c502.php3.

PHILLIPS, James G., 2006. The psychology of internet use and misuse. In: ANANDARAJAN, Murugan, Claire A. SIMMERS a Thompson S. H. TEO. *The internet and workplace transformation*. New York: Routledge, 41-62. ISBN: 0-7656-1445-6.

Práce a právo. *Ministerstvo práce a sociálních věcí* [online]. [vid. 2022-9-6]. Dostupné z: https://www.mpsv.cz/prace-a-pravo.

RAJAH, Rashimah a Vivien K. G. LIM, 2018. Cyberloafing in the realm of IoPTS: Examining individual neutralization and organizational citizenship behavior. In: SIMMERS, Claire a Murugan ANANDARAJAN. *The internet of people, things and services: workplace transformations*. New York: Routledge, Taylor & Francis Group, 67-99. ISBN 978-1-315-18240-7.

RAMAYAH, T. Personal web usage and work inefficiency. *Business Strategy Series* [online]. 2010, **11**(5), 295-301 [cit. 2022-10-02]. ISSN 1751-5637. Dostupné z: doi:10.1108/17515631011080704.

ROBINSON, Sandra L. a Rebecca J. BENNETT. A typology of deviant workplace behaviors: A multidimensional scaling study. *The Academy of Management Journal*. 1995, **38**(2), 555-572.

SAO, Ruchi, Shravan CHANDAK, Bhavisha PATEL a Pritam BHADADE. Cyberloafing: Effects on Employee Job Performance and Behavior. *International Journal of Recent Technology and Engineering (IJRTE)* [online]. 2020, **8**(5), 1509-1515 [cit. 2022-10-03]. ISSN 22773878. Dostupné z: doi:10.35940/ijrte.E4832.018520.

SELWYN, Neil. A Safe Haven for Misbehaving?. *Social Science Computer Review* [online]. 2008, **26**(4), 446-465 [cit. 2022-10-03]. ISSN 0894-4393. Dostupné z: doi:10.1177/0894439307313515.

SIMMERS, Claire a Murugan ANANDARAJAN, 2018. Introduction The internet of people, things and services (IoPTS): Workplace Transformations. In: SIMMERS, Claire a Murugan ANANDARAJAN. *The internet of people, things and services: workplace transformations*. New York: Routledge, Taylor & Francis Group, 1-8. ISBN 978-1-315-18240-7.

TOMŠEJ, Jakub. *Zákoník práce 2022 s výkladem: právní stav k 1.1.2022*. Osmnácté vydání. Praha: Grada, 2022. ISBN 978-80-271-3539-4.

WEISSENFELD, Katinka, Olga ABRAMOVA a Hanna KRASNOVA. Antecedents for cyberloafing: A literature review. *14th International Conference on Wirtschaftsinformatik.* 2019, **14**, 1687-1701.

WHITE, Jerod, Tara BEHREND a Ian SIDERITS. Changes in Technology. In: HOFFMAN, Brian J., Mindy K. SHOSS a Lauren A. WEGMAN, ed. *The Cambridge Handbook of the Changing Nature of Work* [online]. Cambridge University Press, 2020, 2020-4-2, s. 69-100 [cit. 2022-10-02]. ISBN 9781108278034. Dostupné z: doi:10.1017/9781108278034.004.

YOGUN, Ayşe Esmeray. Cyberloafing and innovative work behavior among banking sector employees. *International Journal of Business and Management Review*. 2015, **3**(10), 61-71.

Zákon č. 262/2006 Sb., zákoník práce. In: *Sbírka zákonů*.

Seznam obrázků a tabulek

Seznam obrázků

Seznam tabulek

Seznam příloh

Příloha 1 Dotazník

Dobrý den,

touto cestou bych Vás chtěla požádat o vyplnění následujícího dotazníku, který slouží jako výzkumný nástroj mé bakalářské práce věnující se způsobům využívání internetu v práci. Dotazník se skládá z 18 otázek a jeho vyplnění Vám zabere cca. 10 minut. Vaše odpovědi budou zcela anonymní a budou využity pouze k výzkumným účelům této bakalářské práce.

Předem Vám děkuji za spolupráci.

Jarmila Žižková, studentka ŠKODA AUTO Vysoké školy

1. Jste:
   - Žena
   - Muž
2. Uveďte, do které věkové kategorie patříte:
   - Mladší než a včetně 25 let
   - 26 – 35 let
   - 36 – 45 let
   - 46 – 55 let
   - 56 – 65 let
   - 66 a více let
3. Jaký počítač využíváte k výkonu práce?
   - Počítač poskytnutý zaměstnavatelem
   - Soukromý počítač
4. Používáte během pracovní doby zařízení umožňující přístup na internet také k soukromým účelům?
   - Ano
   - Ne
5. Pokud ano, k soukromým účelům používáte? (Zaškrtněte všechna Vámi využívaná zařízení)
   - Počítač (stolní počítač, notebook, laptop apod.) poskytnutý zaměstnavatelem
   - Tablet poskytnutý zaměstnavatelem
   - Mobilní telefon poskytnutý zaměstnavatelem
   - Soukromý počítač
   - Soukromý tablet
   - Soukromý mobilní telefon
6. Připojujete se během pracovní doby k internetu za soukromými účely z vašeho soukromého mobilního zařízení a prostřednictvím Vašich mobilních dat?
   - Ano
   - Ne
7. Používání internetu k soukromým účelům během pracovní doby považuji za:
   - Normální a užitečné
   - Normální
   - Neumím posoudit
   - Nevhodné
   - Nevhodné a škodlivé
8. Považoval/a byste povolení používat internet k soukromým účelům během pracovní doby za důležitý motivační faktor v případě hledání nového zaměstnání?
   - Ano
   - Ne
9. Jak často využíváte přístup k internetu pro soukromé účely během pracovní doby?
   - Nikdy

- Několikrát za měsíc
- 1x týdně
- Několikrát týdně
- Denně

10. Za jakým účelem využíváte přístup k internetu k soukromým účelům během pracovní doby? (Označte všechny Vámi využívané aktivity)
    - Ke vzdělávacím účelům
    - Navštěvování zpravodajských webů
    - Sociální sítě
    - Sociální interakce
    - Online nakupování
    - Online bankovnictví
    - Hraní her
    - Stahování souborů
    - Přístup k soukromým účelům nevyužívám
    - Jiné
11. Využíváte přístup k internetu k soukromým účelům za účelem odpočinku od práce?
    - Ano
    - Ne
12. Myslíte si, že používání internetu k soukromým účelům představuje pro Vaši organizaci riziko z hlediska kybernetické bezpečnosti?
    - Ano
    - Spíše ano
    - Nevím
    - Spíše ne
    - Ne
13. Zúčastnila/a jste se školení, které zahrnovalo informace o pravidlech užívání internetu ve Vaší organizaci?
    - Ano
    - Ne
    - Nevzpomínám si
14. Domníváte se, že opatření k užívání internetu jsou ve Vaší organizaci srozumitelná a jasná?
    - Ano
    - Spíše ano
    - Nevím
    - Spíše ne
    - Ne
15. Jak Vám vyhovuje politika nastavení užívání internetu ve Vaší organizaci?
    - Naprosto vyhovuje
    - Vyhovuje
    - Neumím posoudit
    - Nevyhovuje
    - Naprosto nevyhovuje
16. Pokud jste označil/a v předchozí otázce možnost nevyhovuje/naprosto nevyhovuje, v čem konkrétně Vám tato politika nevyhovuje?

17. Považujete monitoring za potřebný kontrolní mechanismus ve vztahu s využíváním internetu?
    - Ano
    - Ne
18. Považujete blokování webových stránek/domén za nutný bezpečnostní prvek?
    - Ano
    - Ne

ANOTAČNÍ ZÁZNAM

AUTOR	**Jarmila Žižková**		
STUDIJNÍ PROGRAM/OBOR/SPECIALIZACE	**Specializace Řízení lidských zdrojů**		
NÁZEV PRÁCE	**Cyberloafing: Využívání internetu pro soukromé účely během pracovní doby**		
VEDOUCÍ PRÁCE	**doc. PhDr. Karel Pavlica, Ph.D.**		
KATEDRA	**KRLZ - Katedra řízení lidských zdrojů**	**ROK ODEVZDÁNÍ**	**2022**

POČET STRAN	**51**
POČET OBRÁZKŮ	**3**
POČET TABULEK	**2**
POČET PŘÍLOH	**1**

STRUČNÝ POPIS	**Cílem této bakalářské práce je prezentovat přehled aktuálních poznatků týkajících se využívání internetu v pracovním prostředí a analyzovat ve vybrané společnosti vyskytující se formy cyberloafingu. A následně na základě poznatků z teoretické a praktické části formulovat doporučení týkající se opatření užívání internetu v pracovním prostředí.** **Teoretická část práce se nejprve věnuje definici internetu, jeho využití v pracovním prostředí a základním právním aspektům jeho užívání v českém právu. Následně je pozornost věnována definici cyberloafingu, jeho typologii, důsledkům a výchozím předpokladům podílejícím se na jeho výskytu.** **Jak vyplývá z výsledků výzkumu, je vhodné cyberloafing do jisté míry tolerovat, neboť může mít na zaměstnance i pozitivní vliv.**
KLÍČOVÁ SLOVA	**cyberloafing, internet, politika internetu, kybernetická bezpečnost**

ANNOTATION

AUTHOR	**Jarmila Žižková**		
FIELD	**Specialization Human Resources Management**		
THESIS TITLE	**Cyberloafing: Use of the internet for private purposes during working hours**		
SUPERVISOR	**doc. PhDr. Karel Pavlica, Ph.D.**		
DEPARTMENT	**KRLZ - Department of Human Resources Management**	**YEAR**	**2022**

NUMBER OF PAGES	**51**
NUMBER OF PICTURES	**3**
NUMBER OF TABLES	**2**
NUMBER OF APPENDICES	**1**

SUMMARY	**The aim of this bachelor thesis is to present an overview of the current knowledge concerning the use of the Internet in the work environment and to analyse the forms of cyberloafing occurring in a selected company. Following that, based on the findings from the theoretical and practical part, to formulate recommendations concerning measures of Internet use in the work environment.** **The theoretical part of the thesis is first devoted to the definition of the Internet, its use in the work environment and the basic legal aspects of its use in Czech law. Subsequently, attention is paid to the definition of cyberloafing, its typology, consequences and initial assumptions involved in its occurrence.** **As the results of the research show, cyberloafing should be tolerated to a certain extent, as it may have a positive effect on employees.**
KEY WORDS	**cyberloafing, internet, internet policy, cyber security**