Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Internet a Intranet – jejich klady, zápory a využitelnost u Policie ČR

Lucie Semrádová

Česká zemědělská univerzita v Praze | Provozně ekonomická fakulta

Katedra informačních technologií | Akademický rok 2009/2010

ZADÁNÍ DIPLOMOVÉ PRÁCE

Lucie Semrádová

obor Veřejná správa a regionální rozvoj nav.- Cheb

Vedoucí katedry Vám ve smyslu Studijního a zkušebního řádu ČZU v Praze čl. 17 odst. 2 určuje tuto diplomovou práci.

Název práce: **Internet a Intranet - jejich klady, zápory a využitelnost u Policie ČR**

Osnova diplomové práce:

1. Úvod
2. Cíl práce a metodika
3. Internet a Intranet – jejich klady a zápory
4. Využitelnost Internetu a Intranetu Policií ČR
5. Softwarová policie
6. Závěr
7. Seznam použitých zdrojů
8. Přílohy

Rozsah hlavní textové části: 60 - 80 stran

Doporučené zdroje:

1. JIROVSKÝ, Václav. Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Martin Kysela; Petra Tesárková; Miroslav Lochman. 1. vyd. Praha : Grada, 2007. 288 s. ISBN 978-80-247-1561-2.

2. ČERMÁK, Miloš. Internet snadno a rychle : Na Internetu jako doma v devíti krátkých kapitolách. Luděk Bárta. [s.l.] : Moraviapress,a.s., 2002. 43 s.

3. @beceda internetu. Josef Novák; Ludva Vladimír; Jakub Dvorský. 1. vyd. Praha : Computer press , 2000. 78 s. ISBN 8072263692.

4. Zákon č. 140/1961 Sb., trestní zákon, ve znění pozdějších předpisů

5. SMEJKAL, Vladimír, et al. Právo informačních a telekomunikačních systémů. 1 vyd. Praha : C.H. Beck, 2001. 74 s. ISBN 80-7179-552-6.

6. Širokopásmové sítě a jejich aplikace : Moderní komunikační technologie datových a počítačových sítí a jejich aplikace, internet/intranet, WWW, videokonference. Milena Kršková, Radovan Pleva. Olomouc : Poligrafické středisko VUP, 2000. 113 s. ISBN 80-244-0095-2.

Vedoucí diplomové práce: **RNDr. Dagmar Brechlerová, Ph.D.**

Termín odevzdání diplomové práce: duben 2011

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE Provozně ekonomická fakulta

L.S.

.....
Vedoucí katedry

.....
Děkan

V Praze dne: 15. 1. 2010

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Internet a Intranet – jejich klady, zápory a využitelnost u Policie ČR" jsem vypracovala samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autorka uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušila autorská práva třetích osob.

V Praze dne 31. března 2011 _____

Poděkování

Ráda bych touto cestou poděkovala RNDr. Dagmar Brechlerové, Ph.D. za ochotu, cenné připomínky a odborné rady při zpracování této diplomové práce. Dále bych poděkovala panu Bc. Vladimíru Jesínkovi, systémovému pracovníkovi OIKT PČR Karlovarského kraje, za odborné konzultace mi poskytnuté při zpracování teoretické a praktické části této diplomové práce. Též bych ráda poděkovala policistům, zaměstnancům Policie ČR a ostatním osobám za poskytnuté informace a čas věnovaný při vyplňování mých dotazníků.

Internet a Intranet – jejich klady, zápory a využitelnost u Policie ČR

The Internet and the Intranet – their advantages, disadvantages and usage at the Police of the Czech Republic

Souhrn:

Internet a Intranet jsou běžnými a nepostradatelnými nástroji, které mění současný svět. První část diplomové práce je zaměřena na kladné a záporné stránky Internetu a Intranetu, včetně pravidel a zásad, které je vhodné dodržovat, a na portály a projekty zabývající se bezpečností na Internetu. Po teoretické části následuje vlastní výzkum pomocí dotazníku zaměřeného na zkoumanou problematiku. Další část této práce se týká využitelnosti Internetu a Intranetu Policií ČR. Jsou zde popsány internetové policejní stránky www.policie.cz a intranetové policejní stránky. Závěr kapitoly je ukončen opět vlastním výzkumem metodou dotazníkového šetření, který slouží ke zjištění využitelnosti internetového portálu PČR www.policie.cz a Intranetu Ministerstva vnitra „HERMES“ v podmínkách Policie ČR, co je třeba zlepšit a co naopak odstranit za účelem zefektivnění práce. Poslední kapitola pojednává o činnosti softwarové policie a organizacích zabývajících se ochranou autorského práva a práv souvisejících s právem autorským k audiovizuálním dílům a potíráním různých forem pirátství. Jsou zde vysvětleny pojmy porušování autorského práva a softwarové pirátství, včetně rizik a ochrany. Závěr je zakončen statistikou vývoje míry softwarového pirátství.

Summary:

Internet and Intranet are common and indispensable tools that change the world today. The first part of my diploma work is to show what positive and negative pages bring Internet and Intranet, including the rules and principles which are suitable to keep and what portales and projects are deal with security of Internet in nowadays. This whole section is

ended up with own research especially with method of questionnaire investigation. This one is intended for mapped out the situation, whether the common users realize their advantages and disadvantages of Internet and Intranet and also their criminality and netiquette. Another part of this diploma work is concerned how to use the Internet and Intranet of Police of the Czech Republic. There are described the Internet police pages such as www.policie.cz and the Intranet police pages. The conclusion of the chapter is ened up with own research again with a method of questionnaire investigation which it servers at findings of their usage of Internet portal of Police of the Czech Republic www.policie.cz and Intranet of Interior Ministry ¨HERMES¨ in terms of the Police of Czech Republic, saying what is important to make better or remove from these pages for streamlining of work. The last chapter characterizes activity of software Police, the organizations dealing with protection of author´s law with limitation of conception of software piracy, then hazard which is connected by using illegal software and security how to avoid this hazard. The conclusion is ended up with statistics of software piracy.

Klíčová slova

Internet
Intranet
klady
zápory
kriminalita
pravidla slušného chování
bezpečnost
využitelnost
softwarové pirátství
Policie České republiky

Key words

Internet
Intranet
advantages
disadvantages
criminality
rules of ethics
safety
usage
software piracy
Police of the Czech Republic

Obsah:

1. ÚVOD

„Internet je veřejná celosvětová (globální) síť propojující všechny kontinenty, státy, města tak, že jakýkoliv počítač může komunikovat kdykoliv a s jakýmkoliv jiným počítačem, ať se nachází kdekoliv.“[1] „Internet jako celek nikdo nevlastní ani přímo neřídí. Přesto existují instituce podílející se významnou měrou na fungování a dalším rozvoji Internetu. Jako první se jmenuje Internet Society (ISOC), jenž sdružuje internetové uživatele. ISOC má dvě hlavní složky Internet Activities Board (IAB) a Internet Engeneering Task Force (IETF). Obě tyto složky spolupracují s nejvýznamnějšími počítačovými firmami na tvorbě standardů potřebných pro další rozvoj Internetu. Další institucí, která od poloviny roku 1994 dbá na rozvoj služby WWW, je WWW Consorcium (W3C). Neopomenutelnou je i organizace InterNIC dohlížející na přidělování tzv. IP adres počítačů a doménových jmen.“[2]

„Intranet je samostatný uzavřený systém, postavený na obdobných principech jako Internet. Na rozdíl od běžného webu, který je veřejně přístupný, je firemní Intranet zpřístupněn pro uzavřenou skupinu uživatelů, typicky pro firemní zaměstnance.“[3] Jedná se tedy o soukromou síť, jejíž vlastníkem je pouze organizace, která ji provozuje.

[1] *Datacentrum WEDOS* [online].WEDOS Internet, a.s., 26.01.2010 [cit. 2010-10-24]. Co je Internet a jak funguje?. Dostupné z WWW: <http://datacentrum.wedos.com/a/17/co-je-internet-jak-funguje.html>.
[2] *SeniorClub* [online]. 2007 [cit. 2010-10-24]. HISTORIE INTERNETU. Dostupné z WWW: <http://www.seniorclub.cz/internet.htm>.
[3] *PragueBest* [online]. 2010 [cit. 2010-10-24]. Firemní intranet. Dostupné z WWW: <http://www.praguebest.cz/firemni-intranet.html>.

2. CÍL PRÁCE A METODIKA

2. 1 CÍL PRÁCE

Tak jako mince mají svůj rub a líc, tak i Internet a Intranet mají své kladné a záporné stránky. Cílem této práce je:

1. ověřit, zda si běžní uživatelé Internetu a Intranetu uvědomují, jaká pozitiva a negativa mohou tyto dvě sítě přinášet, a s tím spojenou internetovou kriminalitu a bezpečnostní pravidla. Případně navrhnout řešení, která by zjištěné nedostatky odstranila nebo alespoň zmírnila.

2. ověřit, zda a jak policisté a civilní pracovníci Policie ČR využívají pro výkon své služby/práce internetový portál www.policie.cz a Intranet Ministerstva vnitra „HERMES“, v čem spatřují jejich nedostatky nebo co by naopak zlepšili. Následně na základě zjištěných informací navrhnout řešení, která by vedla k zefektivnění práce.

3. poukázat na existenci softwarové policie a dalších organizací monitorující softwarovou kriminalitu, na druhy softwarové kriminality, zejména na charakteristiku a vývoj softwarového pirátství.

2. 2 METODIKA PRÁCE

Pro zpracování této práce bylo nejdříve nutné prostudovat odbornou literaturu zabývající se danou problematikou a zákony spojené s internetovou a softwarovou kriminalitou. Další údaje byly zjišťovány pomocí veřejně dostupných zdrojů na Internetu a Intranetu. Užitečné informace byly též získány i na Oddělení informační a komunikační technologie a Oddělení hospodářské kriminality Policie ČR. Poté bylo provedeno vlastní vypracování, tzn. vytvoření a zaslání dotazníků určených jednak pro běžné uživatele sítě Intranet a Intranet a jednak pro policisty a civilní pracovníky Policie ČR. Následně

odpovědi byly vyhodnoceny, zpracovány do grafů a tabulek a definovány klíčové problémy s návrhy řešení.

3. INTERNET A INTRANET – JEJICH KLADY A ZÁPORY

Tato část práce je zaměřena na historii Internetu a Intranetu, jak obě tyto sítě fungují, na jejich kladné, záporné stránky a bezpečnostní pravidla a zásady, včetně realizace vlastního výzkumu.

3. 1 HISTORIE

3. 1. 1 INTERNET

Internet, tak jak ho známe dnes, je poměrně mladý. Jeho historie je spojena s americkou armádou. V druhé polovině 60. let Američané hledali způsob, jak propojit důležitá vojenská pracoviště a zajistit funkční výměnu informací i v situaci válečného napadení. Řešení představovalo mnohonásobné propojení jednotlivých počítačů pomocí metody zvané dynamické trasování. Prvotní síť ministerstva obrany USA vznikla roku 1969 a jmenovala se ARPANET, podle pracoviště ARPA (Advanced Research Project Agency). Na rostoucí ARPANET se napojovaly i civilní instituce, takže vojáci si později oddělili svou část (MILNET) a zbytek dali k dispozici univerzitám. Této sítě se ujal Národní vědecký fond (NSF – National Science Foundation). Projekt dostal název NSFNET. V druhé polovině 80. let už existovalo podobných sítí víc a postupně se s NSFNETem slučovaly. Nejoblíbenější služba Internetu, World Wide Web, vznikla až roku 1989 ve Švýcarsku, v evropském centru pro jaderný výzkum CERN. Její otec TIM Bernes-Lee ji původně zamýšlel jako vnitropodnikový informační systém. Ve stejném roce byly do Internetu začleněny také Bitnet a Usenet. Z počátku – v roce 1993 – bylo na Internetu pouhých 43 webových adres. Dnes se jejich počet uvádí v sedmimístných číslech.[4]

Historie Internetu v České republice se začíná psát počátkem roku 1990. V té době v bývalém Československu neexistovala žádná pevná linka, vyjma telefonních, a tak se první pokusy o vytvoření počítačové sítě děly pomocí komutovaných linek veřejné telefonní sítě. V březnu 1990 se do naší republiky dostává síť FIDO a následně v květnu

[4] ČERMÁK, Miloš. *Internet snadno a rychle : Na Internetu jako doma v devíti krátkých kapitolách*. Praha : Moraviapress,a.s., 2002. 43 s.

pak síť EUnet, která propojovala zejména Unixové stanice. V říjnu roku 1990 se k nám dostává evropská odnož sítě Bitnet, nebo-li síť EARN (European Academic and Research Network), která již vyžaduje trvalé spojení po pevných okruzích. Prvním uzlem této sítě u nás, a současně i tzv. národním uzlem sítě EARN pro tehdejší Československo, se stal střediskový počítač IBM 4381 na Oblastním výpočetním centru (OVC) ČVUT Praha (nyní VC ČVUT). Síť EARN přitom poskytovala pouze služby dávkového charakteru (zejména elektronickou poštu a přenos souborů), takže vystačila i s relativně pomalými pevnými okruhy. Uzel CSEARN proto začínal s linkou o přenosové rychlosti 9600 b/s, kterou byl připojen na rakouský národní uzel sítě EARN v Linzi.[5] První pokusy s připojením do Internetu se objevují až v listopadu roku 1991. Toto datum je také v různých oficiálních i neoficiálních statistikách uváděno jako datum připojení tehdejšího Československa k Internetu. Zpočátku šlo pouze o komutované napojení z Prahy, později byla k připojení použita pevná linka do Linze, uměle „rozpůlená“ tak, aby jedna její polovina přenášela provoz v rámci sítě EARN a druhá provoz Internetu. 13. února 1992 dochází na ČVUT Praha ke slavnostnímu aktu formálního připojení Československa k Internetu.[6]

3. 1. 2 INTRANET

„Intranet začal vznikat ve stejné době jako první akademické sítě (např. ARPANET v r. 1969), což bylo ještě před vznikem samotného Internetu. První intranetové stránky představovaly stránky se statickým obsahem. Vznikla myšlenka vytvořit privátní stránky, které by se zobrazovaly jen v chráněných oblastech serveru, rozdělit obsah a vytvořit jednoduché profily přiřazující uživatelům přístupová práva a tedy určující, kdo kam může a co smí vidět.

Dnes většina větších i menších podniků používá nějaké účetní, finanční či komplexnější podnikový systém, založený na webových technologiích. Spousta firem dnes považuje za nejdůležitější část systému databázi, ve které je uložena většina jejich informací. Podnikový systém může být tvořen jako klientská aplikace dotazující se do databáze, ale stejně tak může fungovat podnikový informační systém založený na

[5] *Radim Chlad (xchlad@fi.muni.cz)* [online]. 2000 [cit. 2010-10-24]. Historie Internetu v České republice. Dostupné z WWW: <http://www.fi.muni.cz/usr/jkucera/pv109/2000/xchlad.htm>.
[6] *EXTRA.NET* [online]. 2007 [cit. 2010-10-24]. Historie Intranetu. Dostupné z WWW: <http://i-extra.net/it/internet-a-site/historie-internetu/>.

webových technologiích. A právě Intranet je jeden ze způsobů přístupů k datům. Z pohledu uživatele je Intranet prostředí, ve kterém se chová stejně k mnoha různým informačním zdrojům. V praxi to znamená, že si ze stejného prostředí klidně objedná pizzu, vyhledá nové telefonní číslo známého a zároveň naplánuje práci svým podřízeným tak, aby byl efektivněji využit jejich čas.“[7]

3. 2 PRINCIPY FUNGOVÁNÍ

3. 2. 1 INTERNET

Internet je celosvětová síť počítačů. Počítače připojené do Internetu však nejsou stejné, naopak – obsahují různý hardware, operační systémy a software. Je však nutné, aby tyto počítače spolupracovaly. Stejně jako ve svém počítači můžeme mít spoustu různých zařízení, které se však připojují k několika standardním portům nebo slotům, bylo nutné stanovit podobné standardy i pro komunikaci. Tyto standardy se nazývají protokoly. Nejznámějším protokolem je TCP/IP (Transmission Control Protocol/Internet Protocol), který používá k identifikaci čtveřici čísel z intervalu 0-255. Existují další protokoly fungující „nad“ obecným TCP/IP, které zajišťují vzájemnou komunikaci programů spuštěných na těchto počítačích. Každý protokol náleží určité internetové službě. Posíláme-li elektronickou poštu, využívá se elektronická poštovní služba a program, který se obecně nazývá e-mailový klient. Prohlížíme-li si webové stránky na Internetu, využívá se služeb WWW nebo také webu. Chceme-li stáhnout z Internetu nějaká data, například instalační soubor, obrázky nebo film, využívá se někdy internetové služby zvané File Transfer Protocol (FTP) a pro tento účel se používá klient FTP. Různé protokoly tedy znamenají různé internetové služby a tyto služby mohou znamenat různé programy, jejichž prostřednictvím služby Internetu využíváme. Trend poslední doby však centralizuje všechny uvedené služby do jednoho programu od jednoho výrobce – v jednom balíčku dostaneme jak prohlížeč, tak e-mailového klienta a klienta FTP. Takové „balíčky“ jsou např. Internet Explorer nebo Nestcape Communicator.[8]

---

[7] *Referáty-seminárky.cz* [online]. Universita Pardubice : 2007 [cit. 2010-10-24]. Intranet. Dostupné z WWW: <http://referaty-seminarky.cz/intranet/>. ISSN 1802-422X.

[8] NOVÁK, Josef; VLADIMÍR, Ludva; DVORSKÝ, Jakub. *@beceda internetu*. Vyd. 1. Praha : Computer press , 2000. 78 s. ISBN 8072263692.

3. 2. 2 INTRANET

Intranet je založen na stejné infrastruktuře jako Internet. TCP/IP (Transmission Control Protocol/Internet Protocol) jako komunikační protokol, internetové služby (webové servery) a webové prohlížeče jako univerzální přístupový prostředek. Firma ani soukromá osoba při zprovoznění vlastního Intranetu nepotřebuje mít přístup k Internetu. V podstatě jedinou podmínkou je propojit počítače do sítě, např. pomocí switche, a nainstalovat na některý z počítačů servery. Nejlépe je ovšem jeden počítač jako server vyčlenit, hlavně ve větších sítích, a pouze na něm provozovat servery (služby). Základem je tzv. webový server. Ten umožní provozovat vnitřní intranetové stránky přes prohlížeč. Tyto stránky jsou pak uloženy nejčastěji na tomto počítači a slouží třeba jako zdroj informací pro celou firmu. Intranetové stránky bývají zpravidla dostupné z vnitřní sítě. Samozřejmě nic nebrání tomu zpřístupnit je i světu. Zde je ovšem již nutné připojení k Internetu. Též je možné nainstalovat i další služby, např. emailový server, který umožní rozesílání e-mailů v podnikové síti, ftp server, který usnadňuje přenos souborů a jabber server, nebo-li instantní messaging. Typickým obsahem Intranetu bývají interní podnikové informace, jako jsou pravidla, postupy, dokumenty a formuláře.[9]

3. 3 KLADY

3. 3. 1 INTERNET

Kladnou stránku Internetu představuje především:

- ***elektronická komunikace***

V posledních dvou desetiletích dochází ke značným proměnám na poli prostředků pro mezilidskou komunikaci, jejichž společným jmenovatelem je především Internet. Vedle tradičních technologií, jako je telefon nebo klasická pošta, jsou nyní k dispozici i technologie nové, jako např. videokonference, chatování, sociální sítě.

[9] *Wikipedie : Otevřená encyklopedie* [online]. 2009, poslední změna: 29. 8. 2010 v 10:26. [cit. 2010-10-24]. Intranet. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Intranet>.

❖ ***seznamování přes Internet***

Seznamování může mít své klady i zápory. Základem je dobře sepsaný inzerát. Mělo by být bráno zábavnou formou, neboť při prvním setkání se nemusí potkat zrovna ten pravý, ale je šance se seznámit s prima kamarádem. Kladem je též, že dopisovat si můžeme doma u počítače, lze to kdykoliv ukončit, je šance poznat nové lidi atd. Na druhé straně vznikají rizika jako např. že se seznamující osoba stává terčem legrace, chybí neverbální projev (řeč těla, pohybů, gesta, hlas) aj.[10]

❖ ***Internet jako celosvětové informační médium***

Internet spojuje všechna média (TV, rádio, noviny, časopisy knihy) a jejich přednosti (např. velký výběr informací, anonymita, sociální včlenění), slučuje je a přidává k nim i výhody další (např. trvalá dostupnost, decentralizace, aktualizovatelnost, bezprostřední možnost komunikace a zpětné vazby, oboustrannost).[11]

❖ ***cena***

Nejedná se o cenu připojení, ale o cenu informací, které lze na Internetu najít. Tyto informace a služby jsou většinou poskytovány zdarma.

❖ ***volně stahovatelné programy typu freeware a shareware***

Není překvapující, že na programově solidně vybaveném počítači převyšuje cena programů nad cenou počítače. Je to zapříčiněno tím, že ceny programů neklesají tak rychle jako ceny počítačů. Naštěstí i zde může vypomoci Internet. Na něm lze nalézt stránky s obrovským množstvím programů. Jde o programy typu freeware a shareware, které jsou nabízeny buď zdarma, nebo za malý poplatek. Programy bývají rozděleny do několika kategorií podle oblasti použití. Z nich lze pak vybírat programy podle našich požadavků. Na některých WWW stránkách bývají přidány i popisky a hodnocení. Nejlepší programy dokonce dostávají ocenění (tzv. sharewarové Oskary), které svědčí o kvalitě programu.[12]

---

[10] PRAVDOVÁ, Eliška; JEŽKOVÁ, Zuzana. *Máma a já* [online]. 22.07.2009 [cit. 2011-01-02]. Jak se chytí láska v síti. Dostupné z WWW: <http://www.mamaaja.cz/ActiveWeb/Article/1496/jak_se_chyti_laska_v.html>.

[11] NOVÁKOVÁ, Daniela. *Měšec.cz* [online]. 2. 7. 2003 [cit. 2011-01-02]. Nakupujte přes Internet!. Dostupné z WWW: <http://www.mesec.cz/clanky/nakupujte-pres-internet/>. ISSN 1213-4414.

[12] *IReferáty.cz* [online]. 2005 [cit. 2010-10-24]. Internet. Dostupné z WWW: <http://ireferaty.lidovky.cz/309/1208/Internet>.

❖ ***virtuální vzdělávací prostředí (VLEs, LMS)***

Virtuálním vzdělávacím prostředím se rozumí online portál nebo stránky, které fungují podobně jako školní třída. Nabízí studentům vzdělávací obsah věnovaný různé problematice spolu se souborem úkolů a testů, které ověřují úroveň zvládání učiva. Dále může obsahovat nástěnky, chat nebo jiný internetový záznamník. Každý student má svůj individuální účet, pod kterým se do systému přihlašuje.[13]

❖ ***snadné a pohodlné nakupování***

Nakupování přes Internet je velmi pohodlné. Je-li doma nebo v práci počítač, může se nakupovat kdykoli 24 hodin denně, 365 dní v roce. Odpadají tak problémy s parkováním, čekáním u pokladny, blouděním mezi regály v obchodě a dalšími strastmi nákupů. Celý nákup tak lze obstarat z pohodlí domova a hlavně bez zbytečného stresu. Elektroničtí obchodníci často nabízejí mnohem širší nabídku než „kamenný obchodník" a navíc s přidanou hodnotou – např. dodání až do domu (kanceláře), výhodnější cenu, větší dostupnost informací o zboží a podobně.[14]

❖ ***internetové bankovnictví***

Všechny banky na českém trhu mají alespoň jeden kanál přímého bankovnictví, je jím Internetbanking. Banky tuto formu obsluhy nabízejí klientům, aby jim nabídly jistý komfort obsluhy účtu na dálku, ale i nižší poplatky za transakce provedené na účtu. Lze zde zadávat příkazy k úhradě, povolení, změnu či zrušení inkas, měnit a rušit trvalé příkazy, zobrazit historii pohybů na účtu, zůstatek na účtu, zdarma pořizovat elektronické výpisy. Pro internetové bankovnictví platí, že se každý dostane ke svému účtu kdykoli a odkudkoliv na světě v běžném internetovém rozhraní. Dá se nazvat moderní bankovní službou, jejíž využívání je navíc u každé banky cenově zvýhodněno oproti obsluze účtu přes přepážku na pobočce a klient má svůj účet neustále pod kontrolou.[15]

---

[13] *Bezpečí* [online]. 2008, poslední změna: 5.6. 2008 [cit. 2010-10-24]. Internet a kyberšikana . Dostupné z WWW: <http://cms.e-bezpeci.cz/content/view/36/63/lang,czech/>.

[14] NOVÁKOVÁ, Daniela. *Měšec.cz* [online]. 2. 7. 2003 [cit. 2011-01-02]. Nakupujte přes Internet!. Dostupné z WWW: <http://www.mesec.cz/clanky/nakupujte-pres-internet/>. ISSN 1213-4414.

[15] *IDNES.cz : Finance* [online]. 2005 [cit. 2010-10-24]. Co všechno umí internetové bankovnictví. Dostupné z WWW: <http://finance.idnes.cz/viteze.asp?r=viteze&c=A050427_162054_viteze_zal>.

❖ ***Internet jako pomoc pro zdravotně postižené***

Po využití ve vojenství, průmyslu, vědě, školství si našel cestu i k handicapovaným spoluobčanům. Tento fakt úzce souvisí s rozvojem technických možností Internetu, vznikem aplikací a elektronických zdrojů pro osoby s handicapem, rozšířením a snadnější dostupností výpočetní techniky, síťového připojení, zlepšením počítačové gramotnosti, nabídkou speciálních pomůcek ovládaných počítačem či jej ovládajících. Internet může handicapovaným osobám otevřít nové obzory v získávání vědomostí, nového zaměstnání, kontaktů, přátel, v poznání vlastního sebeuplatnění a zvýšení sebedůvěry. Lze se spojit s lidmi s podobnými problémy, hledat pomoc, řešení krizových životních momentů, nebo si pouze jen tak popovídat s někým, kdo je právě připojený a je ochotný poslouchat.[16]

3. 3. 2 INTRANET

Výhodou Intranetu je:

❖ ulehčená komunikace (např. elektronická pošta, diskusní fórum) a zefektivnění práce (zaměstnanci již nemusí data pracně fyzicky vyhledávat v šanonech),

❖ zvýšená informovanost zaměstnanců (interní směrnice, oběžníky) a možnost dalšího vzdělávání (e-learning). Informace jsou dostupné ihned po zveřejnění všem zaměstnancům.

❖ zpětná vazba vůči vedení a podpora pocitu firemní sounáležitosti mezi zaměstnanci,

❖ nástroj informační podpory managementu

V případě, že jsou na Intranetu umístěna počítadla návštěvnosti jednotlivých stránek či sekcí, může intranetový systém pracovat zároveň i jako kontrola efektivnosti a využívání systému. Poté má manažer či IT pracovník možnost vyhodnotit nejčastěji navštěvované sekce zaměstnanci a též si může zobrazit čas tam strávený. Díky tomu získá přehled o aktuální pracovní náplni a odborných zájmech pracovníků. Výhodou je mimo jiné, že

[16] KACHLÍK, Petr. *Pedagogická fakulta Masarykovy univerzity v Brně : katedra speciální pedagogiky* [online]. 2005 [cit. 2011-01-02]. Handicapovaní a Internet . Dostupné z WWW: <http://natura.baf.cz/natura/2003/2/20030205.html>.

vedoucí pracovník může mít přehled nad množstvím vytvořených a vložených dokumentů pracovníky na Intranet. Dokonce je možné zavést i hodnocení vložených dokumentů ostatními zaměstnanci, například formou různých dotazníků či anket. Manažer má možnost hodnotit účast pracovníků v odborných a diskusních skupinách, dále sledovat jejich odezvy na dotazy ostatních zaměstnanců.

- sdílení dat a informací jednotným způsobem

Veškeré informace jsou kdykoliv přípustné na místě, na které budou uživatelé zvyklí. Není nutné řešit sdílení dokumentů elektronicky, nasdílenými disky atd. Odpadá nutnost řešení aktualizace a archivace.

- přidaná hodnota pro zaměstnance v podobě užitečných informací (doprava, tipy pro volný čas) a zábavy,

- přehled o docházkách, dovolených, služebních cestách zaměstnanců,

- spolupráce např. s účetními, pokladními nebo skladovými programy,

- úspora času a nákladů,

- interní nakupování,

- přijímání vstupních dat z různých dalších systémů, které umožňují výstupy ve strukturovaných formátech, např. XML nebo CSV, a dále pak s nimi pracovat. Stejně tak Intranet může exportovat data pro různé systémy v různých formátech. Výstupem mohou být různé tiskové sestavy, různé formáty pro další aplikace atd.

- získávání nových pohledů na firemní data a to díky databázi statistických údajů, firemních formulářů, logotypů. [17]

[17] *FG Forrest* [online]. 2009 [cit. 2010-10-24]. Intranety. Dostupné z WWW: <http://www.fg.cz/cs/nabidka/webova-reseni/intranety.shtml>.

3. 4 ZÁPORY

3. 4. 1 INTERNET

Přes nespornou řadu kladných stránek má Internet i stránky záporné:

❖ ***neaktuálnost, anonymita a velké množství informací***

Pro zveřejňování na Internetu neexistuje žádné povolovací nebo schvalovací řízení či oznamovací povinnost. Mnohé z veřejně přístupných informací jsou anonymní, kdy těžko se dá ověřit jejich původ a důvod zveřejnění. Dále veřejně přístupné informace jsou mnohdy neaktuální. Při použití vyhledávacích nástrojů často dostává uživatel příliš mnoho informací a mezi nimi i mnoho nerelevantních.[18]

❖ ***anonymita chování na Internetu***

Volnost, která v Internetu navozuje dojem anonymity a z ní plynoucí beztrestnost, je zdrojem mnoha nepříjemností. Někteří uživatelé (především e-mailu) se chovají „jako utržení ze řetězu“ a v diskusích nebo reakcích na články zasypávají své oponenty a náhodně čtenáře sprostými výrazy.[19]

❖ ***spamy***

Dříve slovo spam poukazovalo pouze na e-mail, tedy masově odesílaná nevyžádaná elektronická pošta. Dnes je toto slovo rozšířené na celém Internetu. Spam – tedy nevyžádaný obsah – se objevuje i v diskusních skupinách, instant messagingu (ICQ), blozích, návštěvních knihách a na fórech. Nejnovější trend spamu je SMS spam.[20]

❖ ***návody a postupy na výrobu drog nebo výbušnin***

Existují speciální stránky, kde jsou popsány postupy na výrobu drog nebo výbušnin a to především z běžně dostupných materiálů. Jsou převážně v anglickém jazyce a na

[18] *Ústřední knihovna ČVUT* [online]. 2006, poslední změna: 12. 3. 2007 [cit. 2010-10-24]. Další informační zdroje na Internetu. Dostupné z WWW: <http://platan.vc.cvut.cz/vychova/vyuka-fs/zdroje.html>.
[19] *IReferáty.cz* [online]. 2005 [cit. 2010-10-24]. Internet. Dostupné z WWW: <http://ireferaty.lidovky.cz/309/1208/Internet>.
[20] *@Bezpečný internet.cz* [online]. 2009 [cit. 2010-10-24]. Spam. Dostupné z WWW: <http://www.bezpecnyinternet.cz/zacatecnik/e-mail/spam.aspx>.

stránkách, na které se lze dostat až po nějaké době hledání, ale vždy se najde někdo, který to najde a přeloží.[21]

❖ ***šíření počítačových virů***

„Počítačové viry jsou malé softwarové programy určené k šíření z jednoho počítače do jiného a narušování fungování počítače. Virus může poškodit nebo odstranit data v počítači, využít e-mailovou aplikaci k vlastnímu rozšíření do jiného počítače, nebo dokonce vymazat všechna data na pevném disku. Viry se nejsnadněji šíří v přílohách e-mailových zpráv nebo rychlých zpráv. Mohou být zamaskovány v přílohách v podobě zábavných obrázků, přání či zvukových souborů a videosouborů. Šíří se také stahováním z Internetu. Mohou být skryty v nelegálním softwaru a dalších souborech či programech, které se stahují.“[22]

❖ ***kriminalita prováděná pomocí Internetu***

Dnešní kriminalita pomocí Internetu je vysoce organizovaná, internetoví zločinci se úzce specializují, čile mezi sebou obchodují a vyměňují si zkušenosti. Zde je uveden pouze výčet některých internetových trestných činů, kterými jsou např.:

✓ *Extremismus*

Extremismus je chápán především jako projev nesnášenlivosti doprovázený agresivním jednáním vůči zjevně odlišným jedincům či skupinám. Extremistická hnutí a skupiny prosazují medializaci svých myšlenek velmi těžce a tak využívají Internetu jakožto média „pro všechny“. Neexistuje zde regulace ani cenzura obsahu, každý si zde může říkat a šířit, co chce. Internet je využíván i ke komunikaci mezi jednotlivými národními organizacemi těchto skupin a také se jeho prostřednictvím distribuují CD s extremistickými hudebními nahrávkami. Na českém webu můžeme najít zejména weby popisující antisemitské názory a činnosti neonacistických skupin.[23]

---

[21] *IReferáty.cz* [online]. 2005 [cit. 2010-10-24]. Internet. Dostupné z WWW: <http://ireferaty.lidovky.cz/309/1208/Internet>.
[22] *Microsoft* [online]. 2009 [cit. 2010-10-24]. Co je počítačový virus?. Dostupné z WWW: <http://www.microsoft.com/cze/athome/security/viruses/intro_viruses_what.mspx>.
[23] PAUKERTOVÁ, Veronika. *IKAROS* [online]. 2006 [cit. 2010-10-24]. Elektronická informační kriminalita. Dostupné z WWW: <http://www.ikaros.cz/elektronicka-informacni-kriminalita#l5>. ISSN 1212-5075.

- ✓ *šíření pornografie*

Porno průmysl se vždy dokázal výborně přizpůsobit své době a Internet byl jen dalším prostředkem na cestě hanbatých obrázků k zákazníkovi. Bez porna by nebyl Internet zdaleka takový, jaký je dnes. Ne nadarmo je prostituce označována jako nejstarší řemeslo. V každé kultuře i věku hrál sex významnou roli ve společnosti. Někdy byl naprosto samozřejmou záležitostí, jindy tabu, o kterém se ve společnosti nehovořilo. Modernímu věku lze vděčit v tomto ohledu za velikou otevřenost společnosti a snad nikdy neměl sex a porno tolik volnosti jako dnes.[24]

- ✓ *kyberšikana*

Jedná se o specifický druh šikany. Může mít různou podobu, např. zasílání výhružných a krutých emailů a SMS zpráv, výhružné telefonáty nebo obtěžování přes chat, vytváření webových stránek, které různými způsoby (verbálně, graficky, zvukově…..) oběť šikany uráží a zesměšňují, posílání obrázků, fotografií a video nahrávek spolužákům online, kde je oběť zesměšňována a karikována, vyvěšení pornografických fotografií s tváří obětí na Internetu atd..[25]

- ✓ *internetové podvody*

V současnosti probíhá přechod od relativně primitivní formy trestné činnosti spočívající v zasílání zboží na dobírku k podvodů spojeným s placení platební kartou. K podvodům jsou využívány různé burzy na Internetu (např. Aukro), kde se nabízející registruje dle vlastní vůle, bez kontroly ověřující jeho identitu. Následně nabízí za velmi výhodnou cenu různé zboží, které nemá a ani nechce zaslat.[26]

- ✓ *delikty spojené s porušováním autorského práva*

Freehostingové služby, neveřejné sítě či počítače jednotlivců se v rámci Internetu stávají úložišti softwaru nebo dalších datových souborů, které jsou prostřednictvím Internetu šířeny nelegálně. Ať už nabízejí správci těchto prostorů software, MP3 nahrávky nebo

[24] *Digitálně.cz : Magazín stahuj* [online]. 2009 [cit. 2010-10-24]. Jak porno změnilo internet? 1. díl. Dostupné z WWW: <http://digitalne.centrum.cz/jak-porno-zmenilo-internet-1-dil/>.
[25] *Bezpečí* [online]. 2008, poslední změna: 5.6. 2008 [cit. 2010-10-24]. Internet a kyberšikana . Dostupné z WWW: <http://cms.e-bezpeci.cz/content/view/36/63/lang,czech/>
[26] *Safer : Internet.cz* [online]. 2010 [cit. 2010-10-24]. Za bezpečné prostředí virtuálního světa. Dostupné z WWW: <http://www.saferinternet.cz/>.

videosoubory za úplatu nebo zcela zdarma, páchají trestný čin, protože porušují autorský zákon.[27]

- ✓ *phishing*

Slovem phising se označují podvodné e-mailové útoky na uživatele Internetu, jejichž cílem je vylákat důvěrné informace. Nejčastěji jsou to údaje k platebním kartám, včetně PINu, nebo různé přihlašovací údaje k účtům.[28]

- ✓ *pharming*

Pharming na rozdíl od phishingu využívá technologii zvanou DNS cache-poisoning – otrávení paměti DNS záznamů. Principem pharmingu je modifikace záznamů v lokální paměti IP adres, tzn. místo korektní IP adresy je záznam změněn na podvrženou adresu. Když se pak uživatel pokusí připojit k nějaké stránce, prohlížeč vezme modifikovaný záznam z paměti a na Internetu vyhledá příslušný podvržený server.[29]

- ✓ *hacking*

Hacking lze definovat jako neoprávněný průnik do konkrétního informačního systému provedený zvnějšku, zpravidla ze vzdáleného počítače. Jednotlivé případy incidentů se liší zejména motivací (vzrušení, zábava, msta, zvědavost).[30]

- ✓ *cracking*

Cracking na rozdíl od hackingu bývá užíván v případech, jejichž cílem je počitatelný zisk (respektive, jejichž výsledkem je nevratná škoda). Jedná se o prolamování nebo obcházení ochranných prvků elektronických nebo programových produktů s cílem jejich neoprávněného použití.[31]

---

[27] PROTIVÍNSKÝ, Miroslav. Internetová kriminalita : (Z německých zkušeností). In *Kriminalistika : čtvrtletník pro kriminalistickou teorii a praxi.* 2. vyd. [s.l.] : [s.n.], 2002. s. 1. Dostupný z WWW: <http://www.mvcr.cz/casopisy/kriminalistika/2002/02_02/protivin.html>.

[28] *HOAX.cz* [online]. 2008 [cit. 2010-10-24]. Co je to phishing. Dostupné z WWW: <http://hoax.cz/phishing/co-je-to-phishing>.

[29] PAUKERTOVÁ, Veronika. *IKAROS* [online]. 2006 [cit. 2010-10-24]. Elektronická informační kriminalita. Dostupné z WWW: <http://www.ikaros.cz/elektronicka-informacni-kriminalita#l5>. ISSN 1212-5075.

[30] JIROVSKÝ, Václav; HNÍK, Václav; KRULÍK, Oldřich. *MVCR.cz* [online]. 2005 [cit. 2010-10-24]. ZÁKLADNÍ DEFINICE, VZTAHUJÍCÍ SE K TÉMATU KYBERNETICKÝCH HROZEB. Dostupné z WWW: <http://aplikace.mvcr.cz/archiv2008/bezpecnost/informacni/zakladni_info.pdf>.

[31] JIROVSKÝ, Václav, et al. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* . Vyd. 1. Praha : Grada, 2007. 287 s.
ISBN 978-80-247-1561-2.

3. 4. 2 INTRANET

Pro Intranet je inspirací Internet. Záměrem převzít z internetových technologií bylo to pozitivní, avšak Intranet ovšem převzal také řadu negativních aspektů, a to:

- falešný pocit „bezpečí domova“,

- velmi obtížná kontrolovatelnost každého, pokud se jedná o rozsáhlou intranetovou síť. Zaměstnanci mohou získávat informace nejen nutně pro své potřeby, ale také provádět nějaké operace jménem někoho jiného, pozměňovat data ve prospěch svůj či jiného, získávat (pro někoho) konkurenční výhodu. Následky tohoto jednání mohou způsobit ztrátu konkurenční výhody, poškození zákazníka, poškození práva zaměstnance, negativní vliv na image podniku a v konečném důsledku též finanční ztrátu.

- WWW servery jsou oblíbeným terčem hackerů jak na Internetu, tak na Intranetu. WWW server, budovaný jako intranetový, je po technické stránce řešen stejně jako „internetový“, tedy pomocí stejných komponent. Umístěn je v privátní podnikové síti tak, aby byl dobře přístupný pro „interní“ uživatele. Pro externí uživatele přicházející z Internetu je naopak neviditelný. Jsou zde umístěna data, která mohou mít privátní a důvěrný charakter. Průnik na tento server má prakticky stejné atributy, stejný průběh, stejný výsledek. Intranetové servery nechrání firewally. Intranetové WWW aplikace jsou obvykle řádově složitější než internetové (jsou náchylnější na výskyt chyby) a do provozních databází přistupují obvykle s velmi citlivými daty, která mohou být zneužita.

- problém aktualizace a změn obsahu stránek

  Profil a zájmy uživatelů nejsou neměnné, vyvíjí se v čase. To je žádoucí, neboť se dokládá osobní růst pracovníků. Ovšem odtud pramení základní problém, kterým je aktualizace a změna obsahu stránek. Za účelem zjištění potřeb a zájmů uživatelů a tím uzpůsobení intranetových stránek je žádoucí jejich monitoring. Tím vzniká další problém, a to nezájem pracovníků sdělovat informace o sobě. Uživatelé nejsou ochotni věnovat příliš času specifikací svých zájmů, ani zaškrtávání nejrůznějších políček ve

formulářích na webu. Vnímají tyto činnosti jako ztrátu času. Součástí firemní kultury se pak stává soubor různých pobídkových a motivačních nástrojů.[32]

3. 5 NETIQUETTE

Netiquette je soubor pravidel a zásad slušeného chování v prostředí počítačových sítí a elektronických komunikací. Konkrétní obsah těchto pravidel a zásad se vyvinul v době akademické minulosti Internetu, a bez zásadních změn platí i dnes, kdy je Internet v rukou komerční sféry a používá se i pro komerční účely a na komerční bázi. Pravidla netikety by však měla být dodržována i mimo Internet.[33]

3. 5. 1 INTERNET

Všichni internetoví uživatelé jsou jenom lidé, tudíž i ty nejmodernější technologie a služby si přizpůsobí k obrazu svému. Měli by však respektovat určité zásady:

- „Dodržovat obvyklá pravidla slušnosti normálního života. Co je nevhodné v obvyklém životě, je samozřejmě nevhodné i na Internetu.
- Zjistit taktně, s kým se mluví. Internet je přístupný lidem z celého světa, a v každé zemi platí jiná morálka. Co je dovolené na americkém chatu, nemusí být dovolené na arabském, a to platí o všech podobných skupinách. Politika, náboženství a podobné problémy by proto měly být diskutovány s maximálním taktem a v mezích slušnosti.
- Brát ohled na druhé. Ne každý má tak dobré internetové připojené jako Vy. Někteří se připojují z domu přes modem a draze za to platí. Neposílat proto zbytečně velké e-mailové zprávy.
- I když se píše bez diakritiky, snažit se používat správný pravopis. Dále nezveřejňovat nepravdivé, nebo i pravdivé, ale choulostivé informace. Neporušovat autorská práva.
- Pomáhat v diskuzích. Pokud má někdo v diskuzi nějaký problém, odpovědět mu, pokud je známa odpověď. Někdo jiný může pomoci nám. Platí zásada: „Napřed poslouchej, pak piš“.

[32] HYNEK, J. *Intranet není jen o dokumentech : Moderní řízení*. č.10. Praha : Economia, 2003. 48 s.
[33] PETERKA, Jiří. *EArchiv.cz* [online]. 2008 [cit. 2010-10-24]. Netiquette. Dostupné z WWW: <http://www.earchiv.cz/axxxk160/a705k164.php3>.

- Respektovat soukromí jiných. Pokud omylem přišla zpráva, která Vám nepatří, je vhodné ji smazat a taktně upozornit odesílatele na jeho chybu.
- Nezneužívat svou moc či své vědomosti. Pokud jste správce serveru, máte sice přístup k poště ostatních, ale nemusíte ji neustále kontrolovat jenom tak z nudy, a pokud umíte hackovat, nemusíte to pořád zkoušet.
- Odpouštět chyby ostatním. I Vy je děláte. Nevysmívat se jim a nenadávat za ně.
- Nešířit hoaxy. Zpomalují Internet. Pokud Vám přijde hoax, zdvořile upozornit jeho odesílatele, že takové jednání je nevhodné.
- Nerozesílat spam a reklamu.
- Nestahovat warez.“[34]

3. 5. 2 INTRANET

Jako Internet, tak i Intranet má své zásady, které by měly být uživateli v podniku dodržovány. V rámci Policie ČR a Ministerstva vnitra ČR se jedná o tyto zásady:

- „respektovat pokyny Útvaru systémového řízení a informatiky Policejního prezídia ČR (OSŘI PP ČR) a oddělení informačních a komunikačních technologií na příslušných útvarech, týkající se využívání sítě Intranet,
- po skončení práce na pracovní stanici provést odhlášení a pracovní stanici vypnout nebo ji zajistit proti neoprávněnému použití jiným způsobem,
- neprodleně vypnout pracovní stanici při zjištění závad na pracovní stanici, které by mohly ohrozit bezpečnost nebo funkčnost sítě Intranet (např. napadení virem),
- informovat administrátora lokální sítě o skutečnostech, které by mohly způsobit ohrožení bezpečnosti nebo funkčnosti sítě Intranet, a o zjištění poruchy některé služby sítě Intranet,
- uživatel, kterému bylo správcem uživatelských kont zřízeno uživatelské konto pro přístup k serverům nebo datovým službám v síti Intranet, je povinen:
    - používat přidělené uživatelské konto pro přístup k těm serverům nebo datovým službám serverů, u kterých je vyžadována identifikace uživatele,
    - chránit své uživatelské heslo před možným zneužitím,

[34] *Bezpečně-online.cz* [online]. 2010 [cit. 2010-10-24]. Etiketa, netiketa, chatiketa. Dostupné z WWW: <http://www.bezpecne-online.cz/surfuj-bezpecne/komunikace-se-svetem/etiketa-netiketa-chatiketa/205-3/netiketa>.

- neumožnit ostatním pracovníkům použití svého uživatelského konta při práci v síti Intranet,
- po skončení práce v síti Intranet provést odhlášení uživatele ze sítě Intranet ukončením aplikace Microsoft Internet Explorer,

❖ uživatel na pracovních stanicích nesmí:

- provádět změny v konfiguraci technického a programového vybavení komunikačních prostředků a měnit připojení a přidělenou identifikaci (IP adresu) pracovní stanice vůči počítačové síti, není-li administrátorem lokální sítě nebo správcem počítačových programů,
- instalovat počítačové programy a aplikace, není-li správcem počítačových programů,
- spouštět a provozovat datové služby, které z pracovní stanice vytvoří server, pokud to nebylo stanoveno interním aktem řízení lokálního provozovatele,
- zpracovávat, ukládat, odesílat nebo zpřístupňovat materiály, obsahující utajované skutečnosti,
- připojovat do lokální sítě jiné počítačové sestavy, než které byly připojeny administrátorem lokální sítě,
- žádnými prostředky se pokoušet získat v síti Intranet přístupová práva, která mu nebyla přidělena; pokud chybou získá jemu nepříslušející přístupová práva, je povinen tuto skutečnost neprodleně ohlásit správci uživatelských kont,
- vykonávat takové úkony, které vedou k dlouhodobému zpomalování nebo časovému omezování práce ostatních uživatelů sítě Intranet (například přenášení rozsáhlých datových souborů) mimo dobu, kterou pro tento účel vymezil lokální provozovatel na základě dohody s provozním gestorem, s výjimkou mimořádných případů, kdy je to nezbytně nutné pro plnění služebních nebo pracovních úkolů a hrozí nebezpečí z prodlení; v takovém případě je povinen informovat vedoucího pracovníka lokálního provozovatele.“[35]

[35] Česko. Využívání datové sítě Intranet Ministerstva vnitra „HERMES”. In *Závazný pokyn policejního prezidenta*. 9.8. 2005, 2005, 72, 80, s. 14.

3. 6. BEZPEČNOST NA INTERNETU - PORTÁLY, PROJEKTY

V následující části jsou popsány internetové portály a projekty zabývající se bezpečností na Internetu.

3.6.1 SAFER INTERNET - WWW.SAFERINTERNET.CZ

Safer Internet je národní centrum bezpečnějšího Internetu. Přispívá ke zvyšování povědomí o zásadách bezpečného užívání Internetu, poskytuje poradenství a pomoc. Na internetových stránkách www.saferinternet.cz lze nalézt následující odkazy:

- **horka-linka.cz**

Horká linka je nástrojem boje proti internetové kriminalitě a zneužívání dětí na Internetu (zejména dětské pornografie). V listopadu 2009 byla přijata za člena mezinárodní sítě horkých linek sdružených v organizaci INHOPE.

- **bezpecne-online.cz**

Vzdělávací server bezpecne-online.cz se zaměřuje na děti a dospívající s cílem podporovat u nich bezpečné a sebejisté používání Internetu a nových komunikačních technologií. Tematickým těžištěm je především ochrana uživatelů sociálních sítí a chatů, aktivní ochrana soukromých informací před zneužitím a efektivní využívání možností informačních technologií na Internetu. Kromě osvěty mezi dětmi a teenagery se webové stránky bezpecne-online.cz také zaměřují na učitele a rodiče. Stránky mají za cíl poskytnout učitelům základní metodickou podporu při výuce, rodičům mohou zorientovat se v online světě dětí a v nových technologiích.[36]

- **pomoconline.cz**

„Dětským obětem internetové kriminality pomáhá linka pomoci, která byla zřízena v rámci akreditované sociální služby TKI (telefonické krizové intervence), od 1.1. 2007 Sdružením

[36] *Horkálinka.cz : Bojujeme proti internetové kriminalitě* [online]. 2009 [cit. 2010-10-24]. Horká linka. Dostupné z WWW: <http://horka-linka.saferinternet.cz/>.

Linka bezpečí.“[37] Když se děti na Internetu cítí být obtěžovány, mohou se kdykoliv obrátit pro pomoc na bezplatnou nonstop krizovou linku, na chat nebo e-mailovou poradnu. Linka bezpečí – Pomoconline CZ průběžně realizuje tématické preventivní kampaně zaměřené na děti i rodiče se stěžením sdělením „Na Internetu nikdy nevíš, kdo je na druhé straně“.

- **richardmaproblem.cz**

Tato linka poskytuje rady v případě problémů spojených s výchovou, šikanou, rozvodem aj.

- **protisikane.cz**

„Tyto stránky poskytují informace o rozdílech mezi šikanou a kyberšikanou. Je zde možno nalézt odkazy na české a evropské webové stránky, které se zabývají touto problematikou, dále kontakt na poradnu, kam se může jedinec obrátit, když bude potřebovat pomoci. Stránky proti šikaně jsou součástí evropské kampaně, do které se zapojilo 29 zemí.“[38]

- **mobilstory.cz**

Na stránkách Mobilstory je možné nalézt užitečné rady v oblasti mobilních telefonů, mobilní etiketě, bezpečnosti na Internetu.

Program Safer Internet na rok 2009 – 2013, jehož celkový rozpočet je plánován na 55 mil. €, je zaměřen na podporu využívání Internetu (zejména dětmi a menšinami), boji proti neodvolenému, nechtěnému a škodlivému obsahu a zvyšování všeobecného povědomí v této oblasti mezi rodiči, učiteli a dětmi jako koncovými uživateli. Oproti předcházejícímu programu SaferInternet Plus je boj proti nelegálnímu obsahu rozšířen i na škodlivé chování (např. grooming) a rovněž jsou zohledněny nové typy komunikace jako sociální sítě (např. Facebook, YouTube, Twitter apod.) V rámci programu jsou pravidelně podporovány rovněž tematické sítě, zejména neziskových organizací zaměřeny na ochranu dětí či průzkumy týkající se chování dětí a dospívající mládeže na Internetu či vytváření znalostních bází za účelem přispívat ke zvyšování povědomí o zásadách bezpečného

[37] *Sdružení Linka bezpečí* [online]. 2009 [cit. 2010-10-24]. Telefonická pomoc dětem. Dostupné z WWW: <http://www.linkabezpeci.cz/webmagazine/home.asp?idk=393>.
[38] *Protišikaně.cz* [online]. 2009 [cit. 2010-10-24]. KAMPAŇ PROTI ŠIKANĚ. Dostupné z WWW: <http://proti-sikane.saferinternet.cz/>.

užívání Internetu. Koordinátorem je společnost CZI s.r.o., která řídí Horkou Linku. Partnery projektu jsou neziskové organizace Sdružení Linka bezpečí (řídí Pomocnou linku) a Online Safety Institute (řídí Osvětové centrum a portál Saferinternet.cz).[39]

3. 6. 2 PROJEKT E-BEZPEČÍ

Projekt E-Bezpečí ve spolupráci se SaferInternetem se věnuje zejména osobní bezpečnosti na Internetu a to zejména dětí. Navazuje na dosavadní projekty, které se tomuto tématu věnují. Neomezuje se pouze na informační kampaň, protože to často v případě dětí často nestačí. Informovat o bezpečném používání Internetu je prvním krokem. Druhým krokem je v případě dětí následná kontrola dodržování těchto zásad.

Další oblastí projektu je budování bezpečné zóny, kam jsou zařazeny portály určené dětem a mládeži nebo se věnující jejich problematice, které vycházejí z bezpečnostních standardů. Do nich jsou řazeny tyto zásady:

- dětský portál musí být monitorován, aby byla možnost kontrolovat dodržování základních bezpečnostních zásad,
- portál pro děti musí působit výchovně, měl by být zproštěn od všech jevů, které ve společnosti děti ohrožují, např. agresivitu, vulgarismy apod.,
- portál by měl působit výchovně, tedy propagovat Internet jako aktivního pomocníka pro realizaci reálné zábavy či vzdělání. Nemělo by tedy jít o Internet pro Internet, kde by děti na Internetu jenom bezúčelně zabíjely čas.[40]

Součástí projektu je také diskusní fórum, členěné do několika témat, které slouží k výměně informací. Cílem projektu je též usilovat o legislativní změny, které by vedly k tomu, aby byly z dotací ze státního rozpočtu a z fondů EU podporovány portály pro děti a mládež, které kladou důraz na osobní bezpečnost dětí.

[39] *Safer : Internet.cz* [online]. 2009 [cit. 2010-10-24]. O projektu. Dostupné z WWW: <http://www.saferinternet.cz/o-projektu/538-3>.
[40] *EBezpečí.cz* [online]. 2008 [cit. 2010-10-24]. Bezpečný internet. Dostupné z WWW: <http://www.ebezpeci.cz/projekt.php>.

3. 6. 3 PORTÁL BEZPEČNÝ INTERNET.CZ

25. srpna 2010 byl spuštěn nový portál Bezpečný internet.cz, který vznikl s cílem ukázat mnohá rizika spojená s používáním Internetu a také na způsoby, jak se jim účinně bránit. V současnosti lze najít na Internetu mnoho informací, které se bezpečnosti věnují. Ve většině případů se však jedná pouze o popis konkrétních rizik bez celkového rámce. Velmi často jsou tyto projekty také zaměřené pouze na určitou skupinu uživatelů, například na děti, nebo jsou vázané na produkty konkrétní společnosti.[41]

Portál Bezpečný internet.cz je rozdělen do několika sekcí tak, aby oslovil všechny uživatele Internetu. Běžní uživatelé se na portále dozví, jak zvýšit svoji bezpečnost při užívání sociálních sítí, internetového bankovnictví nebo při tvorbě hesel pro přístup k různým typům účtů. Pro rodiče a jejich děti je zde připraven oddíl zaměřený na prevenci proti kyberšikaně a dalším druhům obtěžování po Internetu. Děti se mohou zábavnou formou v podobně komiksových příběhů seznámit se základními pravidly spojenými s používáním Internetu, učitelé zde najdou zajímavé tipy pro obohacení výuky. Informace jsou průběžně aktualizovány tak, aby poskytovaly odpovědi na nejnovější triky v kyberkriminalitě a nabídly typy, jak používat nejnovější bezpečnostní prvky.[42]

3. 7 VÝZKUMNÁ ČÁST

Můj vlastní výzkum zahrnuje seznam 20 otázek (3 otevřené, 1 polootevřená a 16 uzavřených) zaměřených na zmapování situace, zda si běžní uživatelé Internetu a Intranetu uvědomují, jaké kladné a záporné stránky tyto dvě sítě přinášejí, s tím spojenou internetovou kriminalitu a bezpečnostní pravidla. Dotazováno bylo celkem 50 uživatelů různé věkové kategorie a dosaženého vzdělání. Vše dokumentují tabulky č. 1 - 3. Podmínkou bylo, aby tyto osoby mohly mít přístup k podnikovému Intranetu na pracovišti a Internetu doma nebo na pracovišti. Následně byla provedena analýza, vyhodnocení jejich odpovědí a vše zpracováno do grafů a tabulek.

---

[41] *@Bezpečný internet.cz* [online]. 2009 [cit. 2010-10-24]. O projektu. Dostupné z WWW: <http://www.bezpecnyinternet.cz/o-projektu/default.aspx>.
[42] *Policie.cz : Policie České republiky – KŘP Moravskoslezského kraje* [online]. 2010 [cit. 2010-10-24]. (NE)bezpečný Internet. Dostupné z WWW: <http://www.policie.cz/clanek/ne-bezpecny-internet.aspx>.

Tabulka č. 1 Zkoumaný soubor dle pohlaví

Pohlaví	n	%
muži	25	50
ženy	25	50
CELKEM	**50**	**100**

Tabulka č. 2 Zkoumaný soubor dle věkové kategorie

Věková kategorie	n	%
méně než 30 let	5	10
31 – 40 let	20	40
41 – 50 let	20	40
51 let a více	5	10
CELKEM	**50**	**100**

Tabulka č. 3 Zkoumaný soubor dle dosaženého vzdělání

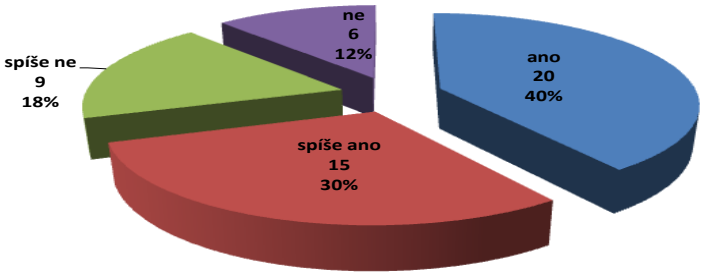
Vzdělání	n	%
ÚSO	3	6
SŠ	27	54
VOŠ	2	4
VŠ	18	36
CELKEM	**50**	**100**

3. 7. 1 VYHODNOCENÍ DOTAZNÍKU

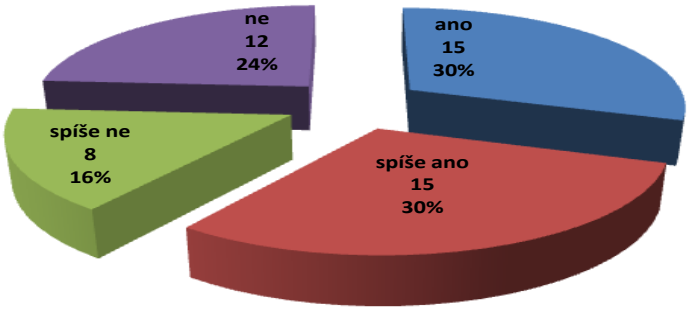
První tři otázky, jak vyplývá z tabulek 1- 3, byly zaměřeny na zjištění základních osobních údajů respondentů. Muži a ženy byli rozděleni na dva stejně velké soubory. Mezi respondenty převládala věková kategorie 31 – 40 let (40% respondentů) a 41 – 50 let (taktéž 40% respondentů). Nadpoloviční většina dosahovala středoškolského vzdělání (54% dotazovaných).

4. otázka: Je pro Vás Internet a Intranet důležitý k životu?

Počet odpovědí dle nabízených možností:



Graf č. 1 Důležitost Internetu v životě



Graf č. 2 Důležitost Intranetu v životě

Na otázku, zda je Internet a Intranet důležitý pro každého z dotazovaných v životě, převažovaly v naprosté většině kladné odpovědi („ano“, „spíše ano“). U Internetu se jednalo o 40% odpovědí „ano“, 30% odpovědí „spíše ano“, u Intranetu o 30% odpovědí „ano“, 30% „spíše ano“. U 12% dotazovaných není Internet důležitý v životě, Intranet pak u 24%.

5. otázka: Jak dlouho používáte Internet a jak dlouho Intranet?

Tabulka č. 4 Četnost odpovědí z hlediska doby používání Internetu a Intranetu

Doba používání	Internet		Intranet	
	n	%	n	%
méně než 1 rok	2	4	4	8
1 - 2 roky	4	8	5	10
2 - 5 let	32	64	29	58
5 - 10 let	10	20	10	20
10 let a více	2	4	2	4
vůbec ho nepoužívám	0	0	0	0
CELKEM	**50**	**100**	**50**	**100**

64% respondentů používá Internet v rozmezí 2 – 5 let, ve stejném rozmezí 2 – 5 let 58% respondentů Intranet.

6. otázka: Kolik hodin denně strávíte na Internetu a kolik na Intranetu?

Tabulka č. 5 Množství denně strávených hodin na Internetu a Intranetu

Množství denně strávených hodin	Internet		Intranet	
	n	%	n	%
méně jak 1 hodina denně	12	24	23	46
1 - 3 hodiny denně	35	70	14	28
3 - 6 hodin denně	2	4	13	26
6 a více hodin denně	1	2	0	0
žádná z nabízených variant	0	0	0	0
CELKEM	**50**	**100**	**50**	**100**

Z 50 dotazovaných osob tráví největší část (35 osob) 1 – 3 hodiny denně na Internetu, na Intranetu je to méně jak 1 hodina denně (23 osob).

7. otázka: Co nejvíce využíváte prostřednictvím Internetu a Intranetu?

Sedmá otázka zaměřená na to, co uživatelé nejvíce využívají na Internetu a Intranetu, byla položena formou volné otevřené otázky, kde každý z dotazovaných mohl uvést 3 příklady. Mezi nejčastější odpovědi v případě Internetu patřila: e-mailová pošta,

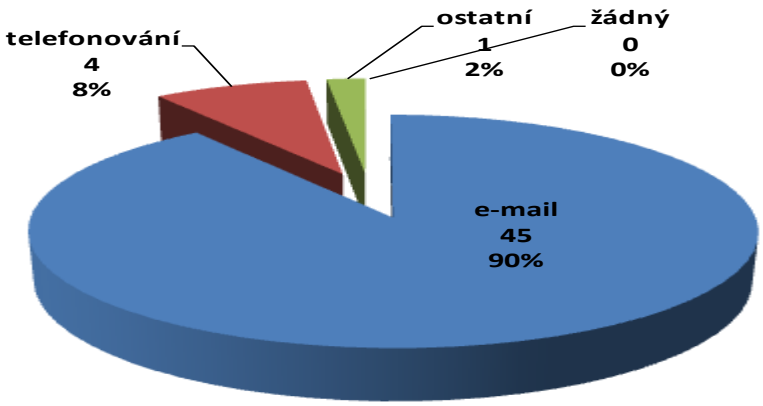
e-shopping, chat, stahování programů a ovladačů, aktuální zpravodajství. V případě Intranetu většina dotazovaných odpověděla, že pomocí jejich podnikového systému využívá elektronickou poštu, informační systémy a aktuální informace.

8. a 9. otázka: Jaké kladné a záporné stránky si myslíte, že přináší Internet a jaké Intranet?

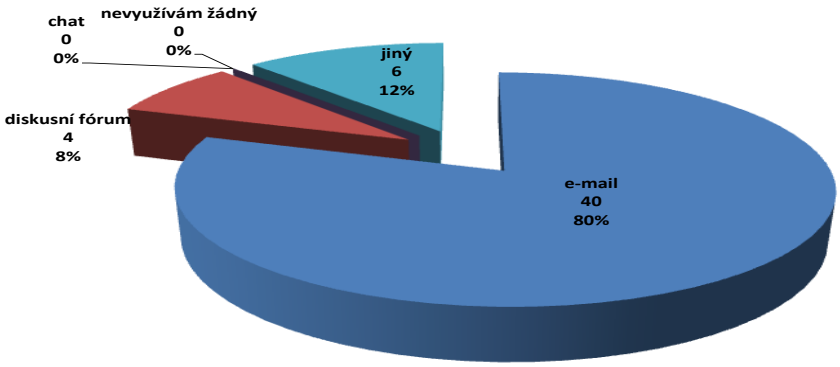
V osmé otázce týkající se kladných stránek a v deváté otázce záporných stránek Internetu a Intranetu, odpověděla většina z dotazovaných, že kladnou stránkou Internetu je především možnost sledovat aktuální informace, získávat velké množství informací rychle a dostupně a v nesporné řadě úspora času a financí. Jako zápornou stránku uvedla ztrátu soukromí, nepřehlednost některých stránek, vyskakovací okna, vtíravou reklamu. Co se týče Intranetu, vidí dotazovaní kladnou stránku především v celorepublikovém propojení, shromáždění informací na jednom místě a elektronickou komunikaci. Zápornou stránkou je dle jejich názoru pomalá rychlost sítě, ne příliš aktualizované informace, místy nepřehledný web a různobarevnost.

10. otázka: Jaký způsob komunikace využíváte nejvíce na Internetu a jaký na Intranetu?

Počet odpovědí dle nabízených možností:



Graf č. 3 Způsob komunikace po Internetu



Graf č. 4 Způsob komunikace po Intranetu

Z nabízených variant využívá nejvíce k internetové komunikaci e-mailovou poštu (90% osob), telefonování jen 8% osob a ostatní způsoby (např. chat, videokonference atd.) 2% osob. V případě Intranetu převládá, tak jako u Internetu, komunikace pomocí e-mailové pošty (80% dotazovaných), diskusní fórum využívá jen 8% dotazovaných a jiný způsob komunikace uvedlo 12 % dotazovaných, kdy se jednalo především o news.

11. otázka: Pracujete pomocí Internetu s choulostivými daty (např. internetové bankovnictví, intimní fotky, burzovní obchody atd.)?

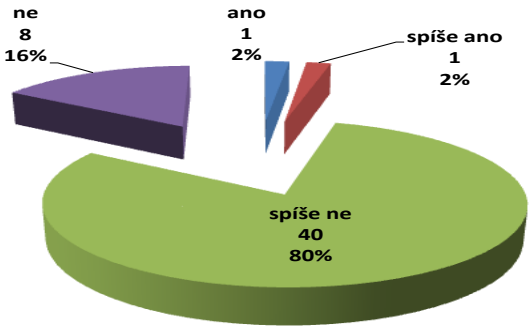
Tabulka č. 6 Práce s choulostivými daty pomocí Internetu

Práce s choulostivými daty pomocí Internetu	n	%
ano, velmi často, důvěřuji všem	0	0
ano, velmi často, ale vždy s maximální opatrností	2	4
pouze v nejnutnějších případech	5	10
ne, nikdy bych přes Internet neposílal choulostivá data	43	84
CELKEM	**50**	**100**

11. otázka orientovaná, zda dotazovaní pracují s choulostivými daty pomocí Internetu a uvědomují si rizika s tím spojená, odpovědělo 84% dotazovaných, že by nikdy přes Internet neposílalo choulostivá data, 10% pouze v nejnutnějším případě a 4% vždy s maximální opatrností.

12. otázka: Bojíte se, že byste se mohli stát terčem nebo účastníkem internetové kriminality?

Počet odpovědí dle nabízených možností:

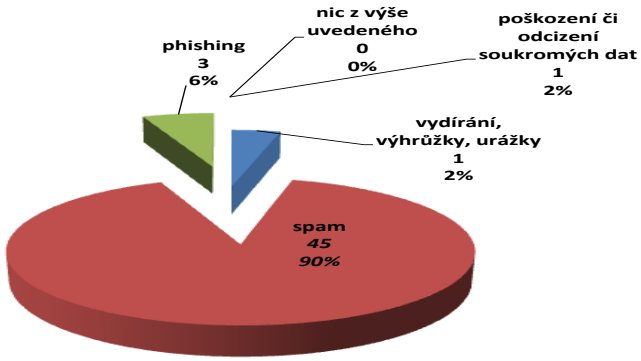


Graf č. 5 Šance stát se terčem či účastníkem internetové kriminality

Na otázku, zda se dotazovaní bojí, že by se mohli stát terčem nebo účastníkem internetové kriminality, většina (80%) odpověděla „spíše ne“.

13. otázka: Stali jste se již někdy terčem nebo se Vám naskytla možnost se stát účastníkem z některých následujících událostí?

Počet odpovědí dle nabízených možností:



Graf č. 6 Varianty událostí internetové kriminality

V návaznosti na předcházející otázku č. 12, byla položena otázka, zda se jimi už někdy stali. Na výběr bylo z 5 možných variant. Téměř každý se stal terčem spamu (90%

dotazovaných) a phishingu 6% dotazovaných, vydírání, výhružek, urážek a poškození či odcizení soukromých dat 2%. dotazovaných.

14. otázka: Z internetových trestných činů se Vám jeví jako nejhorší?

Tabulka č. 7 Nejhorší trestné činy na Internetu

Nejhorší trestné činy na Internetu	n	%
šíření pornografie	18	36
porušování autorského práva	8	16
kyberšikana	18	36
internetové podvody	5	10
jiný (uveďte jaký)	1	2
CELKEM	**50**	**100**

Jako nejhorší z trestných činů po Internetu považuje 36% dotazovaných šíření pornografie a stejné množství i kyberšikanu, za méně důležité pak porušování autorského práva (16% osob) a internetové podvody (10% osob). Jako jiný závažnější trestný čin, než byly nabízené možnosti, uvedla 1 osoba extremistické trestné činy.

15. otázka: Jakým způsobem si opatřujete např. software, filmy, hudbu?

Tabulka č. 8 Způsoby opatřování např. softwaru, filmů, hudby

Způsoby opatřování např. softwaru, filmů, hudby	n	%
kupuji je	3	6
pomocí P2P sítí (např. Torrenty)	11	22
od přátel, známých	4	8
stahuji je zdarma z volně dostupných internetových stránek (freehostingové služby)	32	64
CELKEM	**50**	**100**

Na tuto choulostivou otázku odpověděla většina dotazovaných (64%), že využívá dostupné internetové stránky a stahuje si filmy, hudbu či software zde zdarma, neboť jako důvod uvedli, že je to příliš pro ně drahé či nevidí důvod, proč by měli platit za něco, co lze získat zdarma. Jako další možnou variantu uvedli P2P sítě (22% dotazovaných), příp. je získává od přátel či známých (8% dotazovaných). Jen 6% dotazovaných si software, hudbu či filmy opatřuje koupí.

16. otázka: Jak byste postupně ohodnotili od 1 - 6 rizika spojená s používáním nelegálního softwaru? (1 – nejvíce závažná, 6 nejméně závažná) Jakou považujete nejdůležitější ochranu, abyste rizikům předcházeli?

Tabulka č. 9 Nejvíce závažná rizika spojená s užíváním nelegálního softwaru

Nejvíce závažná rizika	n	%
Trestní postih za používání nelegálního softwaru	28	56
Ztráta dat	7	14
Virové nákazy počítače	8	16
Finanční ztráta	2	4
Ztráta soukromí	3	6
Nemožnost aplikovat bezpečnost a funkční aktualizaci	2	4
CELKEM	50	100

Tabulka č. 10 Ochrana proti rizikům z užívání nelegálního softwaru

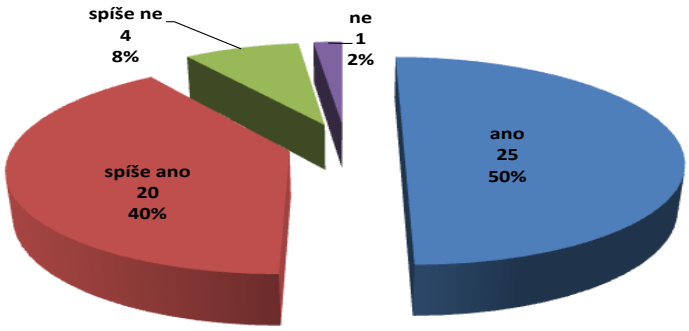
Ochrana proti rizikům	n	%
zakoupení softwaru od autorizovaného prodejce	26	52
zkontrolovat adresu URL webové stránky před poskytnutím informací o kreditní kartě	0	0
při nákupu online zkontrolovat, zda web je pravý pomocí certifikátu zabezpečení	24	48
ani jedna z nabízených možností není vyhovující	0	0
CELKEM	50	100

V návaznosti na předcházející otázku č. 15 byla položena otázka, jakou váhu přisuzují dotazovaní rizikům spojeným s užíváním nelegálního softwaru. Nabízeno bylo 6 variant, k nimž měli dotazovaní přiřadit váhu od 1 – 6 (1 – nejvíce závažné riziko, 6 – nejméně závažné riziko). Jako nejvíce závažné riziko považují, „Trestní postih za používání nelegálního softwaru“ (56% osob), 14% osob „Ztrátu dat“, 16% „Virové nákazy počítače“, 4% „Finanční ztrátu“, 6% „Ztrátu soukromí“ a 4% „Nemožnost aplikovat bezpečnost a funkční aktualizaci“.

Podotázka byla, co považují dotazovaní za nejdůležitější ochranu, aby rizikům předcházeli, odpovědělo 52 % variantu „zakoupení softwaru od autorizovaného prodejce“, 48% variantu „při nákupu online zkontrolovat, zda web je pravý pomocí certifikátu zabezpečení“. Na zbývající 2 varianty neodpověděl nikdo.

17. otázka: Pokud byste chtěli navštívit některé stránky, které nabízejí např. pornografii, xenofobii, rasismus apod., myslíte si, že byste je dokázali najít?

Počet odpovědí dle nabízených možností:



Graf č. 7 Orientace v hledání internetových stránek poskytující zakázaný obsah

Otázka směřována na schopnosti nalézt na Internetu stránky, které poskytují zakázaný obsah, odpovědělo 50% účastníků, že by je dokázali bez problémů najít, 40% spíše ano, 8% spíše ne a 2% by je nedokázala nalézt vůbec.

18. otázka: Jaká zásada slušného chování na Internetu a na Intranetu je pro Vás nejdůležitější, kterou by měl každý člověk dodržovat?

Tabulka č. 11 Nejdůležitější zásada slušného chování na Internetu

Nejdůležitější zásada slušného chování na Internetu	n	%
nepoužívat počítač ke škodě jiného	6	12
nezasahovat do práce druhých lidí	1	2
nepoužívat počítač pro křivé svědectví	1	2
nepoužívat počítač ke krádeži	42	84
CELKEM	**50**	**100**

Tabulka č. 12 Nejdůležitější zásada slušného chování na Intranetu

Nejdůležitější zásada slušného chování na Intranetu	n	%
po skončení práce na pracovní stanici provést odhlášení a pracovní stanici vypnout nebo ji zajistit proti neoprávněnému použití	12	24
informovat administrátora lokální sítě o skutečnosti, která by mohla způsobit ohrožení bezpečnosti nebo funkčnosti sítě Intranet, a o zjištění poruchy některé služby sítě Intranet	3	6
nepřipojovat jiné počítačové sestavy, než které byly připojeny administrátorem	3	6
neumožnit ostatním pracovníkům použít mé uživatelské konto při práci v síti Intranet	32	64
CELKEM	**50**	**100**

V 18. otázce jednoznačně převládala zásada slušného chování na Internetu „nepoužívat počítač ke krádeži“, které přiřadilo největší váhu 84% dotazovaných. 12% dotazovaných pokládá za nejdůležitější zásadu slušného chování „nepoužívat počítač ke škodě jiného“ a shodně 2% „nezasahovat do práce druhých lidí“ a „nepoužívat počítač pro křivé svědectví“. Co se týče zásad slušného chování na Intranetu, zde největší váhu (64%) dosahuje zásada „neumožnit ostatním pracovníkům použít své uživatelské konto při práci v síti Intranet“. 24% dotazovaných se přiklání k zásadě „po skončení práce na pracovní stanici provést odhlášení a pracovní stanici vypnout nebo ji zajistit proti neoprávněnému použití“ a shodně 6% pro každou ze zbylých dvou nabízených zásad.

19. otázka: Který z projektů zabývající se bezpečností Internetu se Vám jeví jako nejlepší?

Tabulka č. 13 Nejlepší projekt zabývající se bezpečností na Internetu

Nejlepší projekt zabývající se bezpečností na Internetu	n	%
Safer Internet	23	46
E-Bezpečí	5	10
Bezpečný internet.cz	7	14
žádný z výše uvedených neznám	15	30
CELKEM	**50**	**100**

19. otázka týkající se projektů zabývajících se bezpečností na Internetu z nabízených variant odpovědělo 46% osob jako nejlepší projekt organizace Safer Internet.

Do popředí staví projekt E-Bezpečí pouhých 10% z dotazovaných a Bezpečný internet.cz 14%. 30% dotazovaných uvedlo, že výše uvedené projekty jsou jim neznámé.

20. otázka: Jaké využíváte programy na zabezpečení?

Tabulka č. 14 Použití programů na zabezpečení PC

Programy na zabezpečení	n	%
freeware (zdarma)	42	84
profesionální komerční programy	0	0
nástroje integrované v systému, např. Microsoft firewall	8	16
CELKEM	**50**	**100**

Na výše uvedenou otázku většina respondentů odpověděla, že využívá k zabezpečení svého PC freeware, a to 42 osob z 50, a zbylých 8 osob nástroje integrované v systému (např. Microsoft firewall). Žádná z dotazovaných osob nevyužívá profesionální komerční programy.

3. 7. 2 ZHODNOCENÍ A DOPORUČENÍ

Po teoretické stránce popsané v první části kapitoly následovalo její ověření v praxi a to metodou dotazníkového šetření. Vytěženi byli běžní uživatelé Internetu a Intranetu. Získané odpovědi byly vyhodnoceny, zpracovány a zjištěno následující:

- **v případě Internetu**

Internet je důležitý pro většinu z dotazovaných, používají ho v průměru 2 – 5 let a tráví na něm denně 1 – 3 hodiny. Nejvíce na této síti využívají e-mailovou poštu, elektronické nakupování, chat, stahování programů a ovladačů a aktuální zpravodajství. Jeho kladné stránky vidí v možnosti sledovat aktuální informace, získávat velké množství informací rychle a dostupně. Další výhodu vidí v úspoře času a financí. Mezi záporné stránky zařadili především ztrátu soukromí, nepřehlednost některých stránek, vyskakovací okna a vtíravou reklamu.

V případě ochrany soukromí je např. doporučeno dbát obezřetnosti při otevírání neznámých emailů, nezveřejňovat nikde osobní údaje. Nepřehlednost, ani vtíravou reklamu nelze odstranit, poněvadž Internet je veřejná síť a zde platí, co kdo si zaplatí, může si zde,

pokud nejde o nezákonný obsah, zveřejnit. Vyskakovací okna je vhodné otevírat pouze na webech, které jsou nám známy.

Co se týče internetové komunikace, využívají dotazovaní nejvíce e-mailovou poštu. Díky tomu se stala většina z nich terčem spamu, nebo-li nevyžádané elektronické pošty masově rozesílané. Řešením a tím i obranou by bylo, kdyby uživatelé zbytečně nezveřejňovali svoji e-mailovou adresu, tzv. neregistrovali se v podezřelých formulářích či soutěžích. Dalším typem obrany by mělo být, aby uživatelé neotvírali jakoukoliv příchozí spamovou zprávu a aby používali aktualizovaný operační systém, antivir a firewall. Proti spamu se lze též bránit právní cestou a to podáním stížnosti k Úřadu pro ochranu osobních údajů.

Z internetových trestných činů se jim nejvíce jevilo jako nejhorší šíření pornografie a kyberšikana. V případě pornografie se lze obrátit na orgány činné v trestním řízení, dětskou pornografii lze navíc nahlásit prostřednictvím projektu Internet Hotline na stránkách www.internethotline.cz. Co se týče kyberšikany, je vhodné si uchovávat veškeré materiály, které danou osobu poškozují, změnit svoji identitu ve virtuálním prostředí či vůbec nereagovat na projevy kyberšikany. Oběť by toto měla oznámit osobám blízkým, příp. se pokusit vypátrat šikanovatele a kontaktovat poskytovatele serveru, který může takové osobě zamezit přístup do domény.

V souvislosti s porušováním autorského práva, což je další nejčastější trestný čin po Internetu, byla položena otázka, jakým způsobem si opatřují software, filmy, hudbu a jak by ohodnotili závažnost rizik z toho vyplývající. Většina dotazovaných uvedla, že si toto zdarma stahují z volně dostupných internetových stránek. Jako důvod uvedli, že se jim koupě softwaru, filmu, hudby zdá příliš drahá nebo nevidí důvod, proč by měli platit za něco, co lze získat zdarma. Za největší riziko pokládali trestní postih z používání nelegálního softwaru. Jako prevenci předcházející těmto rizikům by zkontrolovali při nákupu online web, zda je pravý, pomocí certifikátu zabezpečení. Samozřejmě nejlepší ochrana je koupě softwaru od autorizovaného prodejce.

Většina z dotazovaných by neměla problém nalézt stránky se zakázaným obsahem.

Poslední část dotazníku byla zaměřená na zásady slušného chování a bezpečnost. Tato pravidla jsou nepsaná a nepovinná. Je však vhodné je dodržovat. Jako nejdůležitější zásadu z nabízených variant, kterou je vhodné dodržovat, spatřovalo 84% dotazovaných nezneužívat počítač, tedy i Intranet, k páchání trestných činů (např. krádeži).

K zabezpečení svého PC dotazovaní používají nejvíce freeware a jako nejvýznamnější projekt, zabývající se bezpečností na Internetu, ohodnotili projekt Safer Internet.

- **v případě Intranetu**

Intranet je důležitou součástí života 30 osob z 50 dotazovaných. Využívají ho zhruba 2 – 5 let. Průměrně na něm stráví denně méně jak 1 hodinu. Nejčastěji zde pracují s elektronickou poštou, informačními systémy a seznamování se s aktuálními informacemi.

Za kladnou stránku považují celorepublikové propojení, možnost shromáždění informací na jednom místě a vzájemnou komunikaci mezi odděleními, útvary a podniky.

Jelikož každý podnik má intranetovou síť přizpůsobenou dle svých potřeb, byly rozdílné záporné stránky, které dotazovaní uvedli. Jednotně se však shodovaly jejich názory na pomalou rychlost sítě, ne příliš aktualizované informace, místy nepřehlednost webu a různobarevnost. Řešením by bylo např. aby se dokumenty přijaté v elektronické poště převedly do formátu HTML stránky, uložily se do vhodné databáze a publikovaly se na intranetových stránkách. Tím by se zpřístupnil dokument všem uživatelům a informace se staly aktuálnější. Rychlost sítě lze zvýšit pouze zaplacením odpovídajícího datového okruhu. Podniky mohou vysoutěžit nové poskytovatele datových služeb, kteří poskytnou za stejné peníze lepší podmínky. Nepřehlednost webu a různobarevnost by se dala odstranit vydáním jednotné šablony upravující vzhled podnikových stránek.

Na Intranetu, stejně jako na Internetu, využívají dotazovaní ke komunikaci nejvíce e-mailovou poštu, méně pak již diskusní fórum a zbylých 12% uvedlo jiný způsob komunikace (např. news).

Největší váhu v případě dodržování zásad slušného chování přiřazují „neumožnit ostatním pracovníkům použít své uživatelské konto při práci v síti Intranet“.

4. VYUŽITELNOST INTERNETU A INTRANETU POLICIÍ ČR

Ještě před několika lety nebylo možné informace vůbec poskytnout, neboť neexistovaly požadované informační systémy a komunikace. Dnešním úkolem je vést plošnou osvětu k efektivnímu vytěžování datových fondů, s cílem dosáhnout požadovaných informací v potřebné kvalitě a čase.

Na každém oddělení Policie ČR je k dispozici jedna počítačová sestava, ze které se lze dostat do sítě Internet. Přístup do této sítě je umožněn všem pracovníkům daného oddělení, ovšem musí být dodržována určitá pravidla (např. nestahovat soubory s erotickými stránkami, nechatovat v pracovní době atd.). Internet je využíván jako zdroj velkého množství informací, které napomohou policistovi při vyšetřování trestných činů, dále lze využívat policejní datové schránky a e-mailovou poštu pro komunikaci s vnějším světem. Pracovníkům na oddělení informačních a komunikačních technologií pomáhá Internet při vyhledávání např. vhodných ovladačů pro instalaci.

„Účelem systému Intranet Ministerstva vnitra „HERMES“ je pomocí prostředků výpočetní techniky a komunikační techniky umožnit souběžně více uživatelům (tedy policistům a zaměstnancům Policie ČR) zpřístupnit požadovaná data a vytěžovat textové, datové, grafické nebo multimediální informace uložené na Informačních serverech, aby mohli plnit svěřené úkoly. Uživatelé pro komunikaci využívají elektronickou poštu, mohou se samostatně přihlásit k centrálním datovým bázím a vyhledávat ze svých terminálů potřebné informace z jednotlivých okresů. Obdobně je tomu též i u policejních informačních systémů. Po vytvoření datové sítě a centrálních evidencí (např. Centrální registr obyvatel – CRO, Centrální registr vozidel – CRV) jsou postupně dávány k dispozici rozsáhlé datové fondy policejní veřejnosti. Vše je v závislosti na oprávněnosti i požadavcích jednotlivých pracovišť, přímo na místo výkonu služby.“[43] Při práci s Intranetem musí policisté a zaměstnanci Policie ČR dodržovat bezpečnostní zásady, které jsou upraveny Závazným pokynem Policejního prezidenta č. 80/2005 ze dne 9. srpna 2005. Policie má tu výhodu, že její intranetová síť je jedna z nejobsáhlejších v ČR.

[43] RAK, Roman, et al. *Informatika v kriminalistické a bezpečnostní praxi* [online]. Správa Zpč. kraje Plzeň : Odbor spojení a informatiky MV ČR, 2009 [cit. 2011-01-02]. Dostupné z WWW: <http://kszc-app.ks.zc/oikt/index.html>

4. 1 INTERNETOVÉ STRÁNKY POLICIE ČR

Účelem veřejného WWW serveru Policie ČR je zejména rozvíjení, prohlubování a upevňování pozitivních vztahů s veřejností, využívání vlastního elektronického média a posilování informovanosti široké veřejnosti doma i v zahraničí. V souladu s platnou legislativou (§ 5 odst. 1 zákon č. 106/1999, o svobodném přístupu k informacím, ve znění pozdějších předpisů) poskytují webové stránky informace o organizační struktuře a působnosti, výsledcích, činnosti a aktuálních i připravovaných událostech. Poskytují informace občanovi, jak vyřizovat své záležitosti a na koho se obrátit při podávání dotazů či stížností, informace o volných pracovních místech, veřejných zakázkách, odprodej policejního majetku, preventivní informace, dopravní servis (např. statistiky dopravních nehod, dopravní informace aj.), seznamy adres a odkazů na jednotlivé celorepublikové, územní útvary Policie ČR, Policejní prezídium, Ministerstvo vnitra ČR a Hasičský záchranný sbor ČR.

K dispozici jsou databázové systémy: ***Pátrání po osobách*** – obsahuje informace o všech pohřešovaných osobách, osobách v pátrání; ***Odcizené mobilní telefony*** - obsahem jsou údaje o odcizených mobilních telefonech, které byly zablokovány na žádost majitele policií ve veřejné síti GSM všech operátorů na území ČR); ***Pátrání po vozidlech*** – jedná se o seznam odcizených vozidel, po kterých policie vyhlásila pátrání a vyhledávat lze podle SPZ, čísla motoru, VIN a čísla podvozku; ***Pátrání po uměleckých předmětech*** – zde policie eviduje seznamy odcizených uměleckých předmětů; ***Pátrací oběžník*** – poskytuje pouze aktuální informace o osobách v pátrání, pohřešovaných osobách, může se také týkat odcizených uměleckých předmětů, obrazů, bronzových předmětů atd.; N***eplatné doklady*** - jsou zde vedeny občanské průkazy, cestovní pasy a zbrojní průkazy, které jsou ze zákona neplatné, včetně data ohlášení ztráty nebo odcizení; ***Neplatné služební průkazy*** – databáze obsahuje seznam ztracených služebních průkazů příslušníků PČR, zaměstnanců MV ČR a příslušníků Hasičského záchranného sboru ČR. Údaje mají pouze informativní charakter z důvodu, že může dojít k časové prodlevě mezi ohlášením ztráty nebo odcizení průkazu a zavedením této skutečnosti do informačního systému (cca 24 hodin).

Občan si může na těchto internetových stránkách stáhnout platné právní předpisy, dokumenty, různé manuály (např. protikorupční manuál v boji proti korupci MV ČR), přečíst si aktuální zprávy a novinky policejního charakteru.

Spolupráci policie ČR a EU zajišťuje Kancelář projektů a evropských fondů (KPEF) s určenými policejními útvary. Na jejich internetové stránky se lze dostat prostřednictvím internetového portálu Policie ČR, kde je možnost se dočíst o připravovaných a realizovaných projektech, kontaktních údajích a dalších skutečnostech. Některé dokumenty a databáze (např. Pátrání po uměleckých předmětech) jsou v cizojazyčných verzích – v anglickém, německém a ruském jazyce. Ten, kdo nenašel v hlavní nabídce vše, co potřeboval, může využít podrobný tématický rejstřík hesel, navigační mapu a rubriku Naše tipy. Složitějšímu vyhledávání slouží fulltextové vyhledávání.

4. 2 INTRANETOVÉ STRÁNKY POLICIE ČR

Každý územní odbor Policie ČR (dříve okresní ředitelství) má své intranetové stránky přístupné uživatelům prostřednictvím sítě propojení Ministerstva vnitra ČR na základě přidělených oprávnění. Jsou zde umístěny odkazy na informační systémy, kde za zmínku stojí nově zprovozněný Aplikační rozcestník Praha, nebo-li Elektronická knihovna, jehož obsahem jsou veškeré rozkazy a nařízení, výpisy organizační struktury jednotlivých útvarů a údaje o každé osobě. Dalšími nově zřízenými informačními systémy jsou Elektronická instruktáž, která slouží pro přidělování pokynů vedoucími pracovníky elektronickou cestou; IS KEP určený pro evidenci práce policistů a IS Docházka pro evidenci pracovní doby pracovníka.

Dle rozkazu policejního prezidenta č. 50/2009 byl zaveden bezúplatný dálkový přístup k údajům z katastru nemovitostí prostřednictvím datové sítě Intranet Ministerstva vnitra „HERMES“ a bezpečného prostupu realizovaného Centrálním místem služeb Komunikační infrastruktury. Nyní je možné využívat dvě aplikace. První aplikací je „Nahlížení do katastru nemovitostí“, kterou mohou používat všichni uživatelé sítě Intranet, protože se jedná o aplikaci standardně dostupnou v síti Internet bez uživatelského konta. Druhou aplikací je „Dálkový přístup k údajům katastru“, kterou mohou používat pouze určení pracovníci, kteří jsou oprávněni využívat bezúplatný dálkový přístup k údajům katastru a kterým byl na základě registrační karty zřízen účet.

Na intranetových stránkách jsou umístěny odkazy na centrální a krajské servery, na jednotlivá oddělení v rámci jednoho územního odboru, interní telefonní seznamy, seznamy

advokátů, tlumočníků, znalců, služební pohotovosti a seznamy e-mailových adres pro poštu Exchange a Mail602.

Ve zvláštní kolonce jsou aktuální informace, se kterými by se měl každý seznámit a užitečné informace (např. jízdní řády, jídelníček, předpověď počasí atd.).

Každý útvar si dává požadavky pracovníkům na oddělení informačních a komunikačních technologií, co chtějí na svých stránkách mít zveřejněno. Stránky se obsahově liší podle charakteru útvarů.

4. 2. 1 INFORMAČNÍ SYSTÉMY

Policisté při výkonu své služby využívají informační systémy, které jsou umístěny na intranetových stránkách příslušného územního odboru. Tyto systémy jsou děleny na dvě oblasti:

1.) celostátní policejní evidence vedené v systému dotazy

- ***Schengenský informační systém – SIS***

SIS slouží zejména pro pátrání po osobách (hledaných, pohřešovaných, nežádoucích) a věcech (vozidla, registrační značky, cestovní a osobní doklady, registrační doklady k vozidlům, banky, zbraně a další). Do systému mají přístup všichni příslušníci bezpečnostních sborů členských států na stejné úrovni, jako do svých národních systémů. Doba od vyhlášení pátrání v jednom státě do okamžiku, kdy je tento pátrací záznam dostupný ve všech státech, je maximálně 120 sekund. Systém přispívá k zvýšení efektivity pátrání v schengenském prostoru bez kontrol na vnitřních hranicích.[44]

- ***Informační systém AFIS 2000, C-AFIS, FODAGEN***

„Systém automatizovaného zpracování otisků prstů AFIS 2000 je elektronicky vedenou sbírkou obrazců papilárních linií otisků prstů. Informační systém C-AFIS, který je z IS AFIS 2000 datově odvozen, je počítačově vedenou evidencí osob, které byly podrobeny sejmutí otisků prstů. Tento informační systém obsahuje pouze textové informace, je možné

[44] *Policejní prezidium* [online]. 2009 [cit. 2011-01-02]. Schengenský informační systém – SIS. Dostupné z WWW: <http://mail-inter.pcr.cz/interpol/Sierene/SIS.htm>

jej on-line vytěžovat v rámci resortní datové sítě. Slouží všem složkám policie ke zjištění, zda osoba byla či nebyla daktyloskopována a pod jakým číslem je uložen elektronický obraz jejích papilárních linií otisků prstů. FODAGEN je určen k pořizování, uschovávání a využívání identifikačních úkolů realizovaných kriminalistickými techniky u osob v souvislosti s plněním úkolů policie. Obsahuje evidenci osob, kriminalistických fotografií, popisy osob, záznamy o pořízených daktyloskopických kartách a evidenci odebraných biologických materiálů. Umožňuje oprávněným uživatelům v rámci resortní datové sítě online vytěžovat a aktualizovat data.

❖ ***Informační systém „Evidence dopravních nehod" – EDN***

Systém EDN umožňuje získávání, shromažďování a vytěžování informací o nehodách v silničním provozu na území ČR.

❖ ***Evidenčně statistický systém kriminality – ESSK***

Evidenčně statistický systém kriminality ESSK je celostátní systém, jehož účelem je poskytovat statistické údaje o kriminalitě evidované Policií ČR a MV, o počtu pachatelů trestných činů a ve vymezeném rozsahu o obětech trestné činnosti u vybrané kriminality.

❖ ***Informační systém „Zájmové osoby policie" – ZOP***

ZOP je celostátní policejní informační systém s údaji k osobám, které byly Policií ČR vyšetřovány pro trestný čin a na něž byl zpracován a předložen návrh na podání obžaloby nebo o nichž bylo vyšetřovatelem jiným způsobem v přípravném řízení rozhodnuto jako o pachatelích trestného činu (např. zastavením trestního stíhání pro jeho nepřípustnost), a k osobám pachatelů trestných činů, u nichž je trestní stíhání nepřípustné nebo neúčelné.

❖ ***Informační systém „Neukončené přípravné řízení o známých pachatelích" – AVIZO***

IS AVIZO umožňuje policistům rychle získat informace, zda určitá osoba je v dané době stíhaná na území ČR jako obviněný v etapě přípravného řízení před zpracováním návrhu na podání obžaloby, nebo rozhodnutím příslušného orgánu v přípravném řízení kromě rozhodnutí o přerušení trestního stíhání, nebo informace o osobě, vůči níž jsou příslušnými orgány prováděny úkony trestního řízení před zahájením trestního stíhání jako vůči osobě prokazatelně podezřelé ze spáchání trestního činu, pokud je trestní stíhání nepřípustné nebo

neúčelné a věc nebyla ještě odložena. Údaje jsou získávány ze vstupních údajů IS ESSK (Evidenčně statistický systém kriminality), z nichž se vybírají údaje k osobám, které vyhovují uvedeným kritériím.

- ***Informační systém „Kriminalisticky sledované události" – KSU***

KSU je centrální informační systém kriminalisticky relevantních událostí. Navazuje na více než 10 let provozovaný IS NTS (Informační systém Nápad trestné činnosti), včetně převzetí jeho celostátní databáze, a umožňuje s těmito daty i nadále podle potřeby pracovat. Účelem systému KSU je provádění analytických operací v souvislosti s tzv. „typováním" a zároveň je využíván jako systém k pátrání po odcizených věcech.

- ***Informační systém „Pátrání po motorových vozidlech" – PATRMV***

Centrální informační systém PATRMV je jedním z prostředků pátrání po vozidlech, po kterých bylo na území ČR vyhlášeno pátrání.

- ***Informační systém „Pátrání po osobách" – PATROS***

Informační systém PATROS je jedním z prostředků pátrání po hledaných osobách, pohřešovaných osobách, totožnosti osob a totožnosti nalezených mrtvol a kosterních nálezů.

- ***Informační systém „Evidence uměleckých děl" – SEUD***

Tento systém je určen pro potřeby pátrání po odcizených a nalezených předmětech.

- ***Informační systémy „Stíhané, podezřelé a prověřované osoby" – SPPO, „Deník trestních spisů" – DTS, „Systém osob ve vyšetřování" C-SOV***

Informační systém SPPO je datově odvozen z informačního systému „Deník trestních spisů" DTS. Jeho intranetovou verzi C-SOV je možno vytěžovat on-line prostřednictvím resortní datově sítě. IS DTS je využíván na organizačních článcích služby kriminální policie a vyšetřování pro elektronické monitorování procesních aktivit v rámci trestního řízení. Výstupy z tohoto systému umožňují sledovat množství spáchaných trestných činů v dané oblasti, jejich rozpracovanost, způsob vyřizování apod. Obsahuje data k trestnímu spisu, oznamovateli, k prověřované, podezřelé, stíhané a poškozené osobě, k provedeným

úkonům a k identifikaci zpracovatele trestního spisu. IS SPPO plní funkci rejstříku stíhaných, podezřelých a prověřovaných osob v souvislosti s trestním řízením. Intranetová verze IS SPPO pod označením C-SOV plní funkci orientačního rejstříku stíhaných, podezřelých a prověřovaných osob v souvislosti s trestním řízením. ISC-SOV navíc umožňuje na základě zadání čísla trestního spisu nebo čísla jednacího získat informace o osobách vedených ve spisu s tímto číslem a informace o stavu spisu z pohledu státního zástupce nebo soudu.

- ***Informační systém „TELEFOTO“***

Centrální informační systém TELEFOTO je prostředkem poskytujícím aktuální obrazové informace pro pátrání po pachatelích trestné činnosti s vysokou společenskou nebezpečností, pátrání po hledaných a pohřešovaných osobách, ke kterým jsou hlášena mimořádná opatření, identifikace osob, nálezů mrtvol, pátrání po odcizených věcech velké hodnoty, po odcizených uměleckých předmětech a starožitnostech a pátrání po původu nalezených nebo zajištěných uměleckých předmětů a starožitností.

- ***Informační systém „Událost“***

IS Událost registruje hlášení o stanovených událostech pro potřeby rozhodování a operativního řízení při plnění úkolů Policie ČR, zejména na úseku předcházení a odhalování trestné činnosti, zjišťování pachatelů trestných činů a konání vyšetřování.

- ***Informační systém „Evidence držitelů zbraní“ – D-ZBRANĚ***

IS D-ZBRANĚ je centrální počítačově vedený systém evidence o držitelích zbraní, zbraních, zbrojních průkazech, zbrojních licencích a průkazech zbraní

- ***Informační systém „Evidence trestního řízení“ – ETŘ***

Cílem systému je vedení jednotného protokolu trestných činů, přestupků, čísel jednacích a protokolu událostí, vytváření písemností a zpracování písemných, obrazových, zvukových, případně jiných záznamů neutajovaného charakteru souvisejících s trestním a přestupkovým řízením na úrovni Policie ČR územních odborů a na úrovni správy kraje.[45]

[45] *Praha OSŘI* [online]. 2009 [cit. 2011-01-02]. Informační systémy. Dostupné z WWW: <http://cportal.pcr.cz/inf_sys/prospekty/default.asp>

2.) evidence Ministerstva vnitra

❖ ***Centrální evidence obyvatel – CEO***

CEO je nejzákladnějším a klíčovým informačním systémem civilně-správních agend. Všechny státní informační systémy, které obsahují informace o občanech, navazují na tento informační systém. Slouží pro identifikaci osob. Obsahuje základní údaje o osobě (jméno, příjmení, rodné příjmení, rodné číslo, datum narození, pohlaví), místo narození, trvalého (přechodného) pobytu, místo úmrtí, rodinné a partnerské vazby (rodiče, partnery, děti), stav (svobodný/á, vdaná/ženatý, rozvedený/á, vdovec/vdova). Uchovávají se údaje aktuální i všechny minulé (předchozí příjmení, adresy trvalého i přechodného pobytu atd.).

❖ ***Centrální registr silničních vozidel – CRV***

CRV je datovým fondem správních evidencí. Obsahuje všechna motorová i nemotorová vozidla evidovaná dopravními inspektoráty PČR, kterým jsou přidělovány státní poznávací značky. Je fyzicky propojen s CEO.

❖ ***Centrální registr řidičů – CRR***

V tomto systému jsou evidováni všichni řidiči.“[46]

4. 3 VÝZKUMNÁ ČÁST

Cílem výzkumu je zjistit, zda a jak policisté a zaměstnanci Policie ČR využívají při výkonu své služby/práce internetový portál www.policie.cz a Intranet Ministerstva vnitra „HERMES“ v podmínkách Policie ČR. K tomuto byl použit dotazník skládající se z 15 otázek. Z toho byly 3 otázky otevřené, 2 otázky polootevřené a 10 otázek uzavřených. Dotazováno bylo celkem 30 mužů a 20 žen v rámci Krajského ředitelství policie Karlovarského kraje. Z celkového počtu 50 respondentů se 20% pohybovalo ve věkové kategorii méně jak 30 let, 40% ve věku 31 – 40, 30% ve věku 41 – 50 a 10% ve věku 51 a více. Nejpočetnější skupinu tvořili středoškolsky (42%) a vysokoškolsky (40%) vzdělaní lidé. Poměr mezi muži a ženami vysokoškolsky vzdělanými byl rovnoměrný.

[46] RAK, Roman, et al. *Informatika v kriminalistické a bezpečnostní praxi* [online]. Správa Zpč. kraje Plzeň : Odbor spojení a informatiky MV ČR, 2009 [cit. 2011-01-02]. Dostupné z WWW: <http://kszc-app.ks.zc/oikt/index.html>

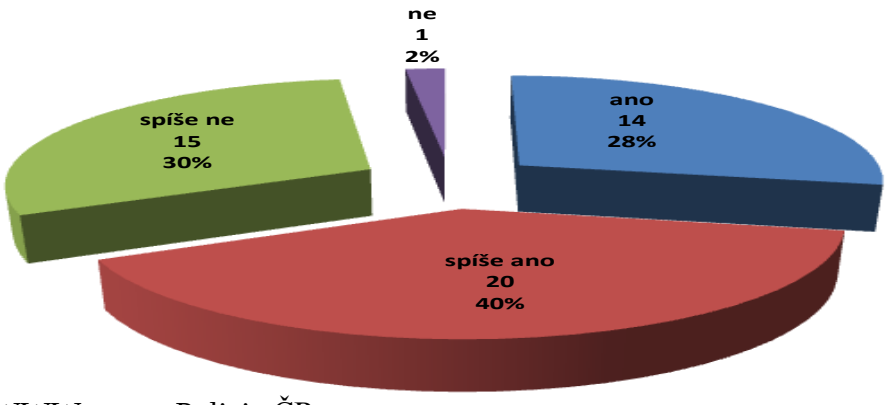
U středoškolsky vzdělaných převažoval poměr žen (62%) nad muži (38%). 10% z dotazovaných bylo na pozici vedoucího pracovníka (z toho 60% ve věku 51 a více), 30% policistů (z toho 67% ve věku 31 – 40), 30% administrativních pracovníků (z toho 73% ve věku 51 a více), 6% zaměstnanců údržby a 4% dotazovaných mělo jiné pracovní zařazení než z nabízených možností.

4. 3. 1 VYHODNOCENÍ DOTAZNÍKU

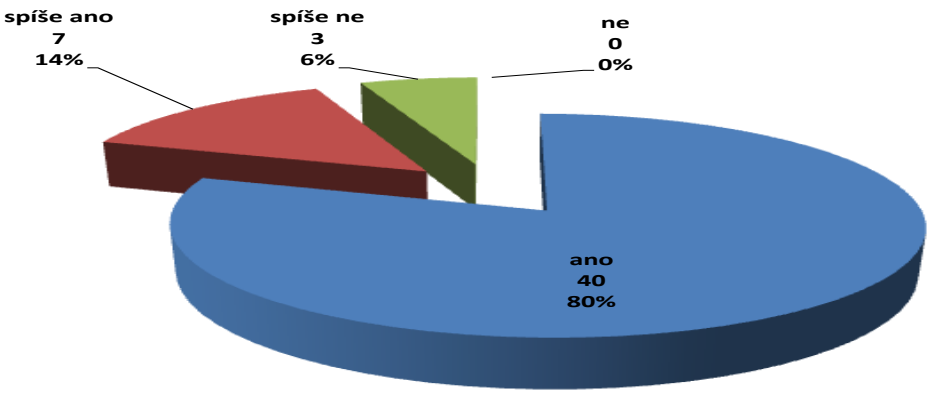
První čtyři otázky byly směřovány na zjištění krátkých anonymních osobních údajů pro lepší validitu dotazníku. Zbytek je již orientován na výše zmíněné téma.

5. otázka: Využíváte při výkonu své služby/práce WWW server Policie ČR a Intranet?

Varianty odpovědí:



Graf. č. 8 WWW server Policie ČR

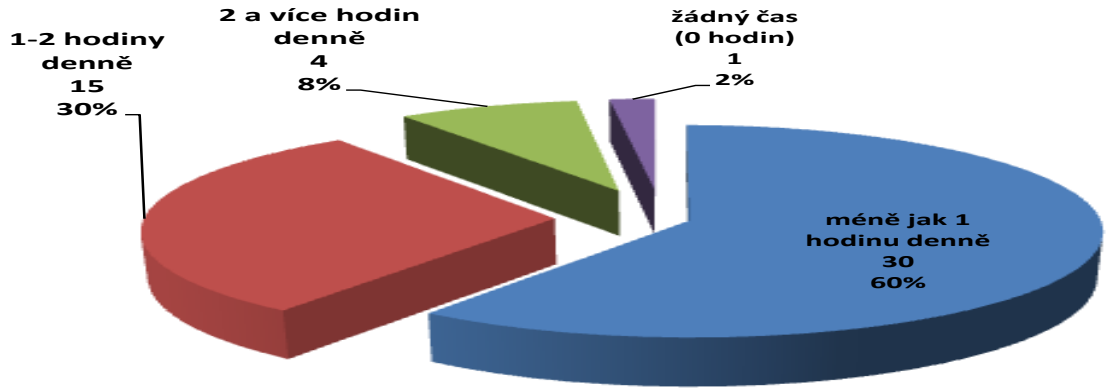


Graf. č. 9 Intranet

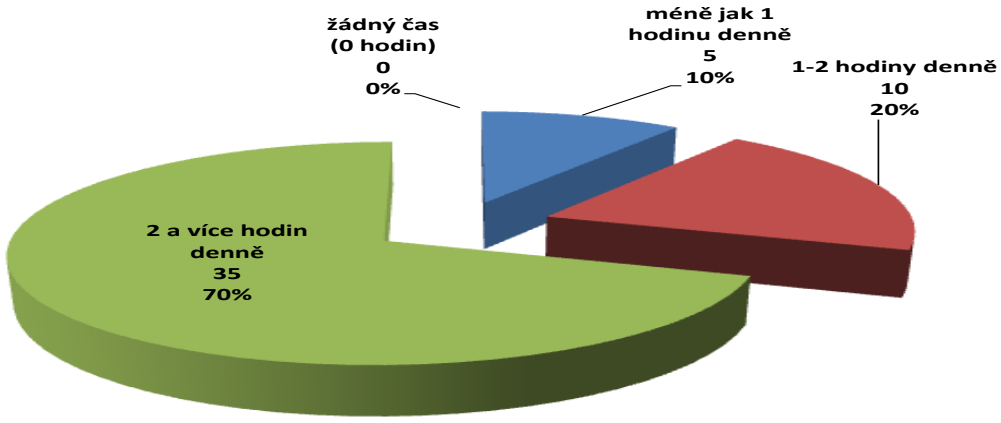
Z nabízených variant využívá při výkonu své služby/práce WWW server Policie ČR 14 respondentů, 20 respondentů spíše ano, 15 spíše ne a 1 respondent ho nevyužívá vůbec. Co se týče Intranetu, 40 dotazovaných Intranet používá při výkonu své služby/práce, 7 spíše ano, 3 spíše ne. Z odpovědí vyplývá, že Intranet je využíván v naprosté většině policisty/zaměstnanci Policie ČR (80%) a WWW server Policie ČR je spíše využíván, avšak ne více jak 40% dotazovanými.

6. otázka: Kolik času strávíte denně na internetovém a kolik na intranetovém portálu PČR?

Četnost odpovědí dle nabízených variant:



Graf. č. 10 Internet



Graf č. 11 Intranet

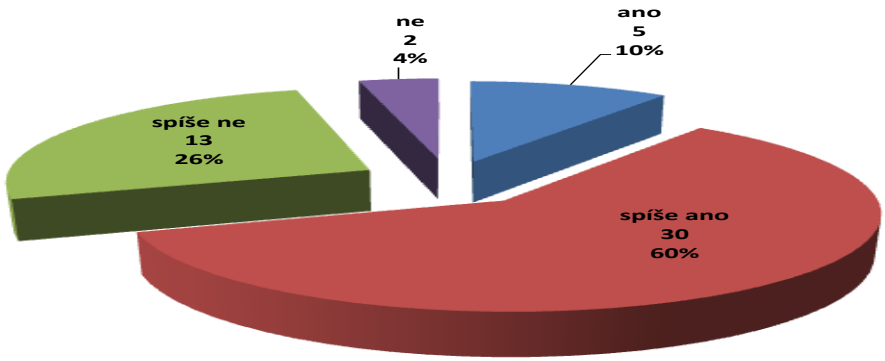
Šestá otázka byla zaměřená na čas strávený na internetovém a intranetovém portálu PČR. Na internetovém portálu tráví z celkového počtu 50 dotazovaných 30 osob méně jak 1 hodinu denně, kdežto na intranetovém portálu, který je v naprosté většině využíván při výkonu povolání, 35 dotazovaných z 50.

7. otázka: Co nejčastěji využíváte na internetových stránkách PČR (www.policie.cz) a co na Intranetu PČR?

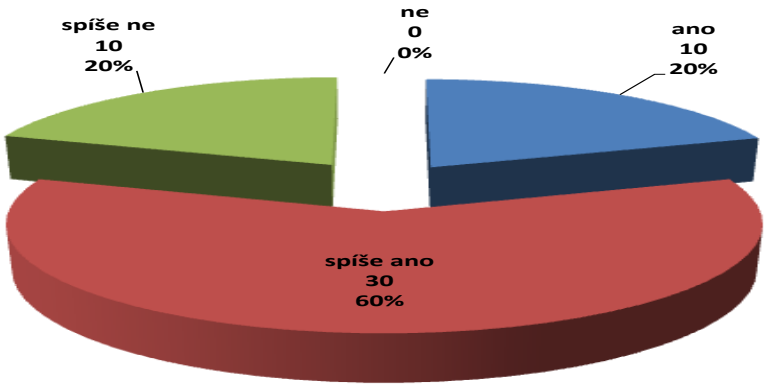
Tato otázka byla položena formou otevřeného dotazování, kde každý respondent mohl uvést 3 příklady, co nejčastěji využívá na internetových stránkách PČR a co na Intranetu PČR. V případě internetových stránek www.policie.cz většina respondentů využívá informační servis, v menší míře pak nabídku volných míst, dotazy a stížnosti, e-podatelnu, akce a projekty. U Intranetu naprostá většina využívá informační systémy, aplikační rozcestník a elektronickou poštu, menší skupina seznam IP adres, telefonní seznam.

8. otázka: Jsou informace na internetových stránkách www.policie cz a na intranetových stránkách PČR aktuální a přehledné?

Počet odpovědí dle nabízených variant:



Graf č. 12 internetové stránky www.policie.cz

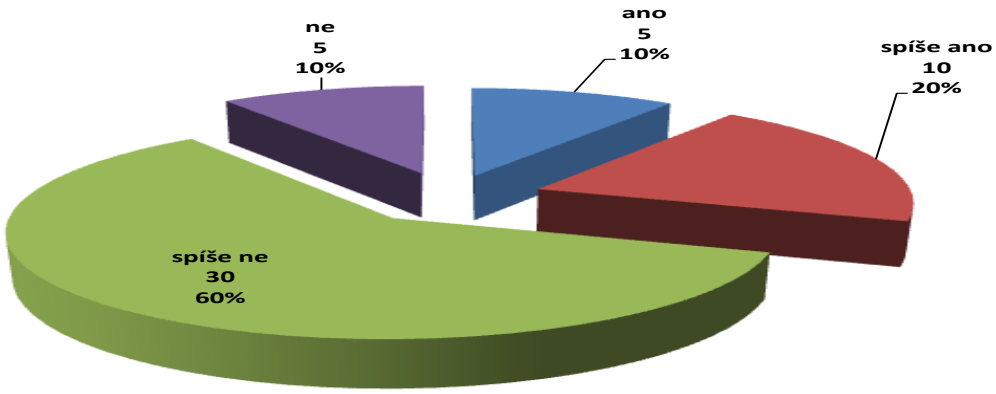


Graf č. 13 intranetové stránky PČR

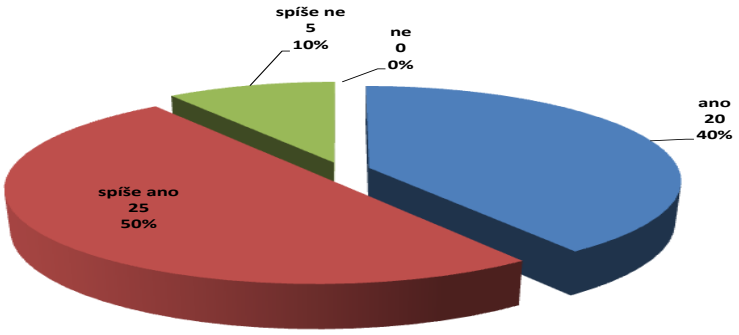
Otázka, která se zabývá aktuálností a přehledností internetových stránek www.policie.cz a intranetových stránek PČR, dopadla shodně, a to 30 odpovědí „spíše ano“. 2 osoby uvedly neaktuálnost a nepřehlednost internetových stránek.

9. otázka: Existuje dobrá provázanost mezi jednotlivými resorty Policie ČR pomocí Internetu a pomocí Intranetu?

Počet odpovědí dle nabízených variant:



Graf č. 14 Internet

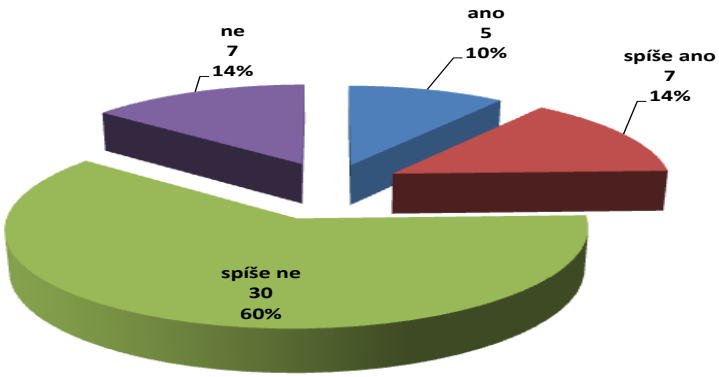


Graf č. 15 Intranet

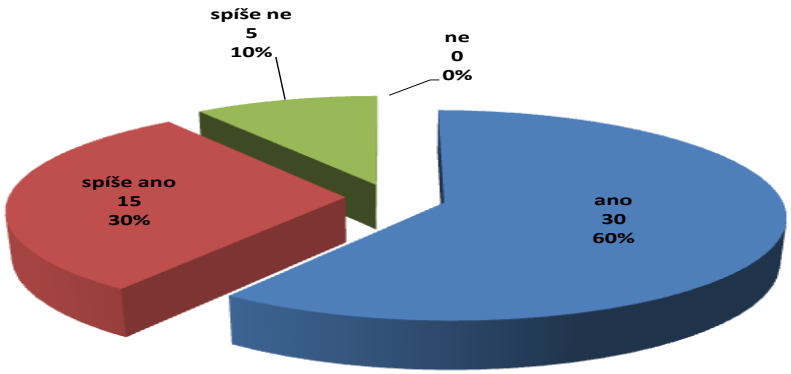
Devátá otázka byla zaměřena na dobrou provázanost mezi jednotlivými resorty Policie ČR pomocí Internetu a Intranetu. 30 lidí odpovědělo, že vidí spíše špatnou provázanost pomocí Internetu, kdežto pomocí Intranetu spíše dobrou (25 osob). 5 lidí jednoznačně uvedlo špatnou provázanost mezi resorty Policie ČR. Tato problematika by měla být řešena.

10. otázka: Využíváte při své práci databázové systémy z internetových stránek www.policie.cz a informační systémy z intranetových stránek PČR?

Využitelnost databázových a informačních systémů:



Graf č. 16 Využitelnost databázových internetových systémů na www.policie.cz



Graf. č. 17 Využitelnost IS na intranetových stránkách PČR

Zde byla položena polootevřená otázka, zda policisté a civilní pracovníci PČR využívají při své práci databázové systémy z internetových stránek www.policie.cz a informační systémy z intranetových stránek PČR. V případě kladných odpovědí, aby uvedli, jaké tři systémy využívají nejvíce. 60% respondentů z celkového počtu 50 osob spíše nevyužívá databázové systémy z internetové stránky www.policie.cz, kladnou odpověď, „ano“ nebo „spíše ano“, uvedlo 26% dotazovaných. Mezi nejčastěji používané systémy byly uvedeny: pátrací oběžník, odcizené mobilní telefony a pátrání po vozidlech. Lepšího výsledku dosahovalo využívání informačních systémů na intranetových stránkách Policie ČR. Zde „ano“ a „spíše ano“ odpovědělo 90% dotazovaných. Jako nejvíce používané systémy uvedly: ETŘ, SUP a BEDRUNKA.

11. otázka: Sledujete pravidelně informace zveřejňované na internetovém portálu www.policie.cz a na policejních intranetových stránkách a jak často?

Tabulka č. 15 Sledování informací zveřejňovaných na internetovém portálu www.policie.cz

Sledovanost informací na www.policie.cz	n	%
ano	5	10
spíše ano	5	10
spíše ne	30	60
ne	10	20
CELKEM	**50**	**100**

Tabulka č. 16 Četnost sledování informací na internetovém portálu www.policie.cz

Četnost sledování informací na www.policie.cz	n	%
velmi často (několikrát denně)	3	6
často (1 x - 2 x týdně)	3	6
méně často (1 x - 2 x měsíčně)	4	8
pouze, pokud jsem k tomu upozorněn/a mým vedoucím	30	60
nikdy	10	20
CELKEM	**50**	**100**

Tabulka č. 17 Sledování zveřejňovaných informací na Intranetu PČR

Sledovanost zveřejňovaných informací na Intranetu PČR	n	%
ano	20	40
spíše ano	20	40
spíše ne	10	20
ne	0	0
CELKEM	**50**	**100**

Tabulka č. 18 Četnost sledování informací na Intranetu Policie ČR

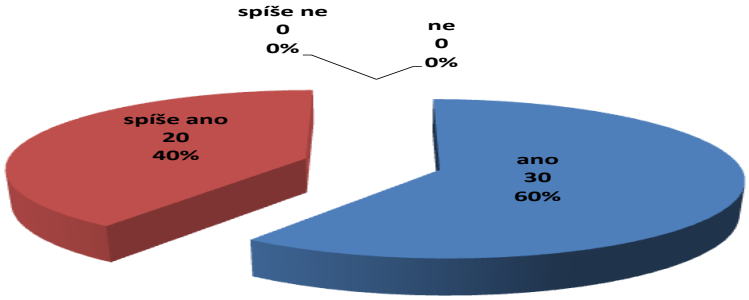
Četnost sledování zveřejňovaných informací na Intranetu PČR	n	%
velmi často (několikrát denně)	20	40
často (1 x - 2 x týdně)	24	48
méně často (1 x - 2 x měsíčně)	3	6
pouze, pokud jsem k tomu upozorněn/a mým vedoucím	3	6
nikdy	0	0
CELKEM	**50**	**100**

V 11. otázce byla položena uzavřená otázka zaměřená na zjištění, zda a jak často policisté a zaměstnanci Policie ČR sledují informace na intranetových stránkách a internetovém portále www.policie.cz. Jak je patrno z tabulek č. 15 a 17 na tuto otázku odpověděla převážná většina u intranetových stránek „ano“ a „spíše ano“, u internetových stránek na www.policie.cz je situace horší, zde většina odpověděla „spíše ne“. Ze zbylých dvou tabulek (č. 16 a 18) je možno vidět četnost sledování zveřejňovaných informací. Informace na internetovém portálu www.policie.cz čte 6% dotazovaných velmi často, 6% často, 8% méně často, 60% pouze, pokud jsou k tomu upozorněni a 20% nečte informace

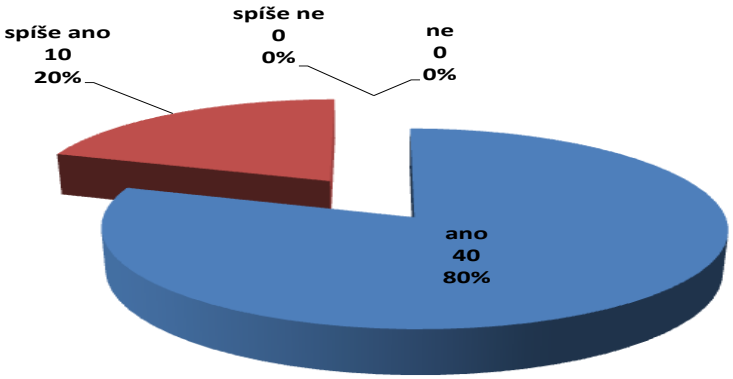
nikdy. Na Intranetu PČR čte zveřejňované informace 40% dotazovaných velmi často, 48% často, 6% méně často a 6% pouze, pokud jsou k tomu upozorněni vedoucím. Poslední možnost neuvedl ani jeden respondent.

12. otázka: Dodržujete bezpečnostní zásady spojené s užíváním sítě internetového portálu www.policie.cz a Intranetu PČR?

Počet odpovědí dle nabízených možností:



Graf č. 18 internetový portál www.policie.cz

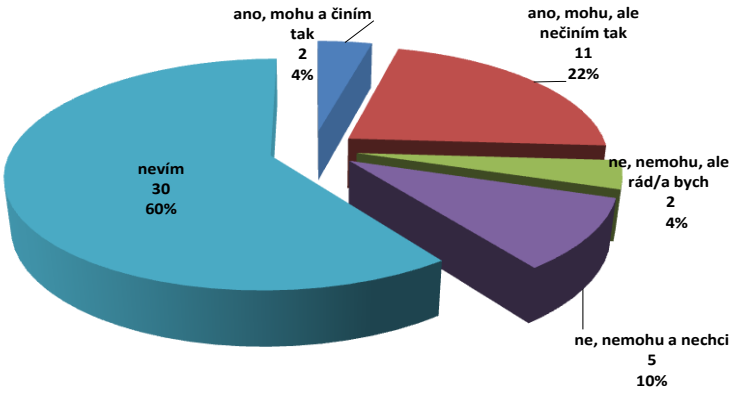


Graf č. 19 Intranet PČR

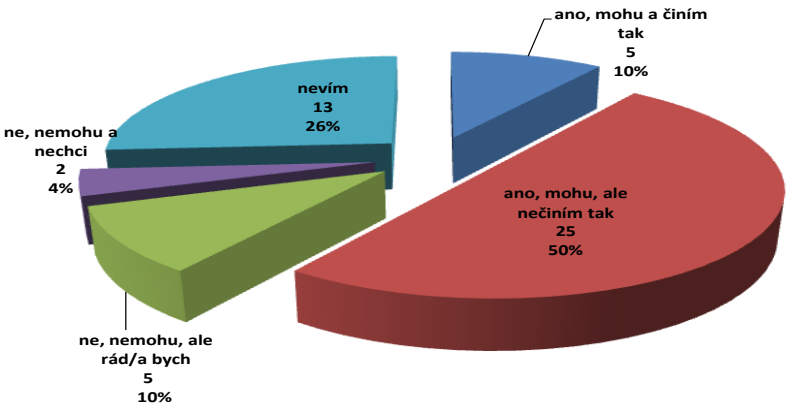
Otázka č. 12 zaměřená na dodržování bezpečnostních zásad u obou sítí byla jednoznačně všemi odpovězena kladně. Shodné byly též odpovědi na uvedení příkladu, jaké zásady dodržují. Jednalo se o aktualizaci antiviru, používání paměťových médií (USB FLASH) zvlášť pro Internet a Intranet, pravidelnou změnu hesla a nikomu toto heslo neukazovat.

13. otázka: Můžete sami navrhovat změny nebo zasílat nápady na zlepšení funkcí internetových stránek www.policie.cz a intranetových?

Počet odpovědí dle nabízených možností:



Graf č. 20 internetové stránky www.policie.cz



Graf č. 21 Intranet PČR

Tato otázka byla zaměřená, zda policisté a zaměstnanci mohou projevovat svoji iniciativu a navrhovat změny nebo zasílat nápady na zlepšení funkcí internetových stránek www.policie.cz a intranetových. V případě internetových stránek www.policie.cz většina dotazovaných neví, zda může či nemůže tak činit. U intranetových stránek je situace lepší,

neboť 25 dotazovaných ví, že může navrhovat změny, ale horší v tom, že tak nečiní. Toto by mělo být řešeno.

14. a 15. otázka: Co byste zlepšil/a na internetových a intranetových stránkách Policie ČR? A co naopak byste odstranil/a?

Poslední 2 otázky nabízely volnou formu, kde každý mohl vyjádřit své názory na zlepšení internetových a intranetových stránek PČR, které jsou zapracovány s mými zjištěními a doporučeními v níže uvedené podkapitole.

4. 3. 2 NÁVRHY A DOPORUČENÍ

Na základě vyhodnoceného dotazníku v kapitole 4.3.1 bylo zjištěno, co by bylo třeba zlepšit a co odstranit pro zefektivnění práce.

V případě internetových stránek www.policie.cz se jedná o:

- **větší aktuálnost** – každý útvar by měl mít možnost sám aktualizovat své informace a policisté a civilní zaměstnanci by se měli samostatně informovat o všem, co je zajímá. V současné době tyto informace vystavují pracovníci Preventivně informačního oddělení, ti však nestíhají. Vzhledem k početním stavům a jejich vytíženosti nemají ostatní útvary na tuto činnost vůbec čas. Do toho vstoupila k Policii ČR také hospodářská krize a tudíž se situace hned tak nezlepší. Možným řešením by bylo vytvoření integrovaného klikacího odkazu, v rámci něhož by se daly nové informace vložit podle stanoveného klíče (např. podle společné integrované databáze jednotlivých úvarů).
- **lepší provázanost jednotlivých resortů Policie ČR** – návrhem by bylo vytvoření uceleného seznamu všech útvarů, pomocí něhož by se daly rychle nalézt hledané útvary
- **odstranit vyskakovací okna** – tento doplněk je opravdu strašný. Je smutné, že mnoho vedoucích pracovníků tuto „zvrhlost“ požaduje. Je to první věc, kterou si většina uživatelů zablokuje na webovém prohlížeči.

- **možnost navrhovat změny, zasílat nápady na zlepšení funkcí** – policisté a zaměstnanci Policie ČR by měli mít možnost zdokonalovat webovou stránku www.policie.cz. Návrhem by bylo obeznámení, jak to mohou učinit, např. zveřejněním v intranetovém Aplikačním rozcestníku. V rámci dotazování někteří policisté či zaměstnanci Policie ČR ani nevěděli, že tyto internetové stránky existují.

V případě intranetových stránek by bylo vhodné:

- **zlepšit přehlednost stránek a organizovanost údajů**, neboť zde chybí jednotná pravidla pro jejich spravování. Měl by být vydán závazný interní pokyn, který by tyto pravidla sjednotil pro všechny útvary. Dalším řešením je zavedení redakčního systému, kterým by se ujednotil obsah a struktura webových stránek. V současné době běží oficiální pilotní projekt redakčního systému SharePointu na Středočeském kraji. Krajské ředitelství policie Karlovarského kraje používá nyní systém z Krajského ředitelství Ústeckého kraje, který je velmi přehledný a hlavně jednoduchý. Jedná se o dynamické ASP stránky s databází SQL. Za zmínku by stál i brněnský systém, který dosahuje podobných kvalit jako ústecký.
- **zvýšit rychlost připojení základních útvarů posílením datových okruhů** – řešením by bylo přejít k jiným poskytovatelům než je O2. Tento je příliš drahý a neposkytuje rychlost za ceny, které může Policie ČR zaplatit. V současné době je již vyřešeno několik útvarů pomocí wifi poskytovatelů. Tato cesta se zdá být přijatelná a vzhledem k rozpočtu Policie ČR na rok 2011 to je asi jediná cesta. Budou se muset volit služby, na které budou finanční prostředky.
- **odstranit mnohobarevnost jednotlivých stránek a zavést uniformní strukturu** – jiná cesta, než vydáním interního nařízení, které by vše upravovalo, není. Tento by měl být vydán v roce 2011.
- **odstranit vyskakovací okna** – jak bylo zmíněno, tento doplněk by nebyl špatný, kdyby byl používán střídmě a s rozvahou, avšak u Policie ČR je tomu opačně.

5. SOFTWAROVÁ POLICIE

Na Internetu i v médiích je často zmiňován termín „softwarová policie“. Jedná se o policejní útvar zaměřený na vyhledávání softwarů a jejich nelegální šíření. „Ve skutečnosti však softwarová policie neexistovala a zkoumání kybernetické trestné činnosti se na počátku 90. let omezovalo pouze na znalecká zkoumání v Kriminalistickém ústavu Praha. V roce 1998 vzniklo pod patronací Policejního prezídia PČR a Úřadu služby kriminální policie a vyšetřování (ÚSKPV) oddělení informační kriminality, které bylo operační a vyšetřovací složkou. Náplní práce oddělení bylo zpočátku softwarové pirátství, ale postupně byla tato problematika přenesena na základní útvary služby kriminální policie a uvedený policejní útvar plní spíše koordinační a informační funkci.

Na počátku roku 2006 vzniklo oddělení informační kriminality. Předpokládá se vytvoření specializovaných míst operativních detektivů na útvarech s republikovou působností a současně na jednotlivých krajských správách PČR. Jako první vzniklo 1. května 2005 pracoviště na PČR, Správě hl. m. Prahy.“[47] „Oddělení informační kriminality se na centrální úrovni zaměřuje na odhalování, vyšetřování a monitorování kriminálních aktivit. Jeho úkolem je zajištění důkazního materiálu na Internetu, servisní činnost a podpora útvarům v rámci ÚSKPV. Jakmile některý z útvarů řeší případ v rámci problematiky informačních technologií, obrací se právě na toto oddělení a dostává se mu odborného servisu a podpory.

Policejní práce probíhá také opačným směrem; odborný poznatek oddělení je předáván dále k šetření podle věcné a místní příslušnosti a trestního řádu. Pouze ve výjimečných, technicky a odborně složitých případech, je tak šetření celého případu vedeno výhradně specializovaným oddělením. Skupina pro informační kriminalitu rovněž zajišťuje vzdělávací aktivity uvnitř PČR a komunikuje s odbornými zahraničními pracovišti. Dále zpracovává poznatky vyplývající z šetření jiných případů, využívá vlastní informátory a přijímá oznámení přímo od občanů.“[48]

[47] JIROVSKÝ, Václav, et al. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* . Vyd. 1. Praha : Grada, 2007. 287 s. ISBN 978-80-247-1561-2

[48] AMBROŽ, Jan. *LUPA.cz* [online]. 24. 5. 2005 6:30 [cit. 2011-01-02]. Jak silná je naše "softwarová policie"?. Dostupné z WWW: <http://www.lupa.cz/clanky/jak-silna-je-nase-softwarova-policie/>.

5. 1 BSA – BUSINESS SOFTWARE ALLIANCE

Informační technologie jsou motorem hospodářského a společenského pokroku na celém světě. Prostřednictvím prozíravé a vyvážené veřejné politiky mohou vlády zvýšit prospěch, který tento prosperující sektor může přinést jak národní, tak globální ekonomice. Mezinárodní organizace Business Software Aliance (BSA) prosazuje po celém světě práva softwarového odvětví. Působí v 80 zemích světa a usiluje o vytváření podmínek pro inovace a růst trhu se softwarem. Vlády a partneři z technologického sektoru spolupracují s BSA na řešení právních otázek a politiky užívání softwaru. BSA zároveň poukazuje na důležitou roli softwarového odvětví pro ekonomický a sociální rozvoj všech zemí světa. Členové BSA každoročně investují miliardy dolarů do ekonomik jednotlivých států. Přispívají k tvorbě nových pracovních míst a vytváření softwarových řešení, která pomáhají lidem po celém světě být produktivnější a lépe a bezpečně navzájem komunikovat. Členy BSA jsou společnosti: Adobe, Altium, Apple, Asseco Poland S.A., Attachmate, Autodesk, Autoform, AVEVA, Bentley Systems, CNC, Corel, Dassault Systèmes SolidWorks Corporation, DBA Lab S.p.A., Mamut, Microsoft, NedGraphics, Progress Software, O&O Software, Scalable Software, Siemens, Symantec, Tekla a The MathWorks. Prezidentem a výkonným ředitelem BSA je Robert W. Holleyman. V čele aliance stojí od roku 1990 a dohlíží na činnost BSA ve více než 85 zemích světa.[49]

5. 2 ČPU - ČESKÁ PROTIPIRÁTSKÁ UNIE

Česká protipirátská unie (ČPU) byla založena v roce 1992 za účelem ochrany autorského práva a práv souvisejících s právem autorským k audiovizuálním dílům a potírání všech forem pirátství v oblasti výroby, dovozu a šíření audiovizuálních děl. ČPU se konstituovala z Protipirátské sekce Unie videodistributorů, který vyvíjela protipirátské aktivity v oblasti audiovize již od počátku 90. let. Činnost ČPU spočívá především v ochraně autorských práv k filmovým dílům, sledování a analýza informací týkajících se autorských práv, přípravě právních kroků proti jejich porušování, spolupráci s orgány činnými v trestním řízení a ostatními institucemi a spolupráci na přípravě nových právních předpisů. V současné době je kladen velký důraz na prevenci a vzdělávání. ČPU sdružuje

filmové a home video distributory a poskytovatele kabelového a televizního vysílání. Na činnosti ČPU se podílí též protipirátské oddělení mezinárodní organizace Motion Picture Association a čestným členem ČPU je Národní filmový archiv. Česká protipirátská unie je zájmovým sdružením právnických osob.

Nejvyšším orgánem České protipirátské unie je valná hromada. Ta je tvořena zástupci všech členských společností a činí základní rozhodnutí týkající se existence ČPU, členské základny, vedení jejích orgánů a její činnosti. Operativní rozhodnutí a kontrolu činnosti a hospodaření vykonává Rada Unie, která se schází jednou za kalendářní čtvrtletí. Členové Rady jsou voleni valnou hromadou. Radě předsedá předseda Rady, který je spolu s ředitelem ČPU statutárním orgánem Unie. Členové rozhodují v orgánech Unie podle počtu hlasů, kterými v rámci svého členství disponují. Předsedou Rady Unie je od 21. 2. 2000 Ing. Ladislav Hrabě, ředitel a předseda představenstva společnosti Bontonfilm a.s.. Ředitelkou České protipirátské unie je Mgr. Markéta Prchalová, která zastává svou funkci od poloviny roku 1997.[50]

5. 3 SOFTWAROVÁ KRIMINALITA

S rozvojem informačních technologií se objevují různé druhy kriminality, např. kriminalita počítačová, internetová, informační, ale také kriminalita softwarová. Softwarovou kriminalitu v České republice převážně monitorují výše zmíněné organizace.

Existují čtyři nejběžnější typy této kriminality:[51]

I. Kopírování koncovými uživateli

Jedná se o obyčejné, nelicencované kopírování jednotlivci nebo podniky. V případě objemových (volume) licencí to může znamenat uvedení menšího počtu počítačů, na které je software instalován.

---

[49] *BSA* [online]. 2009 [cit. 2011-01-02]. Co je softwarové pirátství?. Dostupné z WWW: <http://www.bsa.org/country.aspx?sc_lang=cs-CZ>.
[50] *Česká protipirácká unie* [online]. 2009 [cit. 2011-01-02]. Kdo jsme a čím se zabýváme. Dostupné z WWW: <http://www.cpufilm.cz/kdo_jsme.html>.
[51] *Microsoft* [online]. 2009 [cit. 2011-01-02]. Čtyři nejběžnější typy softwarové kriminality. Dostupné z WWW: <Čtyři nejběžnější typy softwarové kriminality>.

II. Instalování na pevné disky

Toto je praktikováno nepoctivými výrobci počítačů, kteří prodávají PC s předem nainstalovaným nelegálním softwarem. Dealeři používají jednu legálně získanou kopii protiprávně pro instalaci na mnoha počítačích. Disky a dokumentace často chybí nebo jsou nekompletní. Zde je třeba zdůraznit, že jen jediná nelegálně nainstalovaná část operačního systému (jako například soubory IO.sys, MSDOS.sys) je porušením zákona a nelegální instalací softwaru na pevný disk. Někdy jsou nelicencovaným softwarem padělaná média nebo dokumentace, které se pak dodávají koncovým uživatelům, kteří si nejsou vědomi nelegálního původu softwaru.

III. Padělání

Tento druh softwarové kriminality je prováděn většinou ve velkém měřítku, kdy je software a jeho balení nelegálně rozmnožováno – často organizovanými kriminálními skupinami – a pak redistribuováno jako údajně legální produkt.

IV. Falešné kanály

Software je distribuovaný jako speciální zlevněné licence – zákazníkům nakupujícím ve velkém množství, výrobcům počítačů nebo akademickým institucím – který je pak redistribuován dalším uživatelům, kteří tyto licence nevlastní nebo pro ně nejsou kvalifikováni.[52]

5. 3. 1 PORUŠOVÁNÍ AUTORSKÉHO PRÁVA – SOFTWAROVÉ PIRÁTSTVÍ

„Autorské právo je součástí práv plynoucích z „duševního vlastnictví“ a jedná se o specializované odvětví práva zabývajícím se nároky tvůrců autorských děl při využívání jejich tvorby. Prostřednictvím institutu porušování autorského práva v § 152 Trestního zákona č. 140/61 Sb. poskytuje stát autorům chráněných děl ochranu a Autorský zákon jim dává výlučné možnosti rozhodovat o některých aspektech využívání jejich děl. Předmětem autorského práva je dílo literární a jiné dílo umělecké a dílo vědecké, které je jedinečným výsledkem tvůrčí činnosti autora a je vyjádřeno v jakékoliv vnímatelné podobě, včetně

---

[52] *Microsoft* [online]. 2009 [cit. 2011-01-02]. Čtyři nejběžnější typy softwarové kriminality. Dostupné z WWW: <Čtyři nejběžnější typy softwarové kriminality>.

podoby elektronické, trvalé nebo dočasné, bez ohledu na její rozsah, účel nebo význam. Současné autorské dílo musí být pouze jedinečným výsledkem tvůrčí činnosti autora, fyzické osoby, a za dílo nelze považovat zejména námět díla sám o sobě, denní zprávu nebo jiný údaj sám o sobě, myšlenku, postup, princip, metodu, objev, vědeckou teorii, matematický a obdobný vzorec, statistický graf a podobné předměty samy o sobě.

Autorské právo je v České republice ošetřeno autorským zákonem č. 121/200 Sb., který vychází z několika mezinárodních úmluv, zejména tzv. Bernské úmluvy z roku 1886 a Všeobecné úmluvy o autorském právu uzavřené v Ženevě v roce 1952.“[53]

Porušování autorských práv a práv souvisejících s právem autorským je především občanskoprávní delikt, podle okolností ovšem může naplnit znaky skutkové podstaty trestného činu porušování autorských práv, práv souvisejících s právem autorským a práv k databázi podle § 152 Trestního zákona č. 140/61 Sb. nebo přestupku na úseku kultury podle § 32 Zák. č. 200/1990 Sb. o přestupcích. Ochrana a potažmo pirátství se může týkat jak softwaru, tak děl hudebních a filmových, databází i webových stránek. Internet a jeho služby se bezesporu stal stimulem pro masové porušování autorského práva. Na Internetu padají veškeré bariéry a zároveň je prostředím, které poskytuje nepřeberné množství různých pomůcek k překonání ochrany proti kopírování (např. generátory sériových čísel nebo tzv. cracky), návody pro hacking atd.

Softwarové pirátství je synonymem pro neoprávněné užívání softwaru, který je chráněn autorskými právy. K pirátství může dojít při kopírování, stahování, sdílení či prodeji softwaru. Další častou formou pirátství je instalace více kopií softwaru, než umožňuje zakoupená licence. Mnoho lidí si neuvědomuje, že při nákupu softwaru si nekupují vlastní software (program), ale jen licenci na jeho užívání. Tato licence určuje, jakým způsobem lze se softwarem nakládat – např. kolikrát software nainstalovat. Počítačovým programem se nemyslí jen různé kancelářské aplikace, rozmanité utility pro práci s grafikou, ale také hry, které se stávají častou obětí softwarového pirátství u dětí a mládeže.[54]

[53] JIROVSKÝ, Václav, et al. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* . Vyd. 1. Praha : Grada, 2007. 287 s. ISBN 978-80-247-1561-2

[54] *Bezpečný internet.cz* [online]. 2009 [cit. 2011-01-02]. Rizika používání nelegálních programů - softwarové pirátství. Dostupné z WWW: <http://www.bezpecnyinternet.cz/pokrocily/stahovani-souboru-programu/softwarove-piratstvi.aspx>.

5. 3. 2 RIZIKA A OCHRANA

„S používáním nelegálního softwaru jsou spojena tato rizika:

❖ **Riziko trestního postihu za používání nelegálního softwaru**

Používáním nelegálně nabytého softwaru vzniká možnost stíhání za přestupek či trestný čin s následnými sankcemi, které mohou mít podobu peněžitého trestu, trestu propadnutí věci, trestu odnětí svobody až na 5 let podle rozsahu trestného činu. V případě podnikatelů a firem jsou neopomenutelné i doměrky příslušných daní od finančních úřadů, penále z daňových nedoplatků, pokuty, eventuálně pak sankce vyplývající ze živnostenského zákona.

❖ **Riziko ztráty dat**

V nelegálních programech, u nichž není záruka jejich původu, se mohou vyskytovat chyby, které mohou vést k vymazání části nebo všech dat. Tímto lze přijít např. o důležité dokumenty, fotografie a videa.

❖ **Riziko virové nákazy počítače**

Instalací nelegálního programového vybavení z nedůvěryhodných zdrojů hrozí nebezpečí nákazy počítače počítačovým virem. Následné náklady související s jeho odstraněním mohou přesáhnout cenu originálního softwaru.

❖ **Riziko finanční ztráty**

Pokud jsou v počítači uložené citlivé osobní informace nebo je použit počítač k přístupu na bankovní účet, hrozí v případě používání neověřeného nelegálního softwaru průnik do tohoto počítače a zneužití informací s možností přístupu cizí osoby na tento bankovní účet. Vzniklá ztráta může být mnohonásobně vyšší než cena legálního softwaru.

❖ **Riziko ztráty soukromí**

Nelegální software může obsahovat zadní vrátka, která umožní cizí osobě přístup do počítače. Tato osoba může sledovat veškeré aktivity, jež jsou na počítači prováděny, a informace, které takto získá, může zneužít.

❖ **Riziko nemožnosti aplikovat bezpečnosti a funkční aktualizaci**

Výrobci originálního softwaru uvolňují v pravidelných intervalech aktualizace, které zvyšují bezpečnost softwaru a zlepšují jeho funkčnost. V případě nelegálních programů je možnost aplikovat tyto aktualizace omezena nebo zcela znemožněna.“[55]

Těmto rizikům je šance předcházet. Existují tipy, jak se nestat obětí softwarového pirátství, a to:

❖ „software kupovat pouze od renomovaných společností.

❖ při nákupu online se přesvědčit, zda je web pravý. Na tomto webu na stránce, kde se provádí vlastní nákup, se klepne na okraji okna prohlížeče na ikonu zámku a zobrazí se certifikát zabezpečení. Pokud se zámek nezobrazuje, web není pravděpodobně bezpečný.

❖ před poskytnutím informací o kreditní kartě zkontrolovat adresu URL webové stránky. Musí začínat znaky https, ne pouze http. Pokud „s“ chybí, nákup je lepší neprovádět. Písmeno „s“ znamená jen to, že informace jsou při odeslání prostřednictvím Internetu šifrovány. Neznamená to, že web je legitimní.

❖ pokud se zdá, že je cena až příliš dobrá na to, aby mohla být poctivá, tak nejspíš nebude poctivá. Proto je lepší dávat pozor na extrémně nízké ceny a důkladně prověřovat pravost příslušného webu, pokud bude software dodán pouze v bílém obalu

[55] *Bezpečný internet.cz* [online]. 2009 [cit. 2011-01-02]. Rizika používání nelegálních programů - softwarové pirátství. Dostupné z WWW: <http://www.bezpecnyinternet.cz/pokrocily/stahovani-souboru-programu/softwarove-piratstvi.aspx>.

nebo obálce, je pravděpodobně padělaný. Legitimní software je dodán v plastových obalech a s tištěnými pokyny a registrační kartou.“[56]

5. 3. 3 STATISTIKA VÝVOJE MÍRY SOFTWAROVÉHO PIRÁTSTVÍ

Softwarové odvětví bitvu s piráty dlouhodobě vyhrává. Navzdory globální hospodářské krizi tuzemská míra pirátství klesla o procentní bod, a to již druhým rokem (příloha č. 4). Česko se umístilo na 13. místě v celosvětovém žebříčku 20 zemí s nejnižší mírou softwarového pirátství (příloha č. 5). Analýza sleduje užívání nelegálních počítačových programů ve více než stovce zemí světa za rok 2009. Je provedena nezávislou analytickou společností IDC, která se zaměřuje na průzkumy a analýzy v oblasti informačních technologií. Závěry poté zveřejňuje BSA ve své výroční Celosvětové studii softwarového pirátství.[57]

Průměrná míra pirátství v Evropské unii činí 35% a celosvětová 43%. Nejnižší celosvětovou mírou počítačového pirátství se mohou pochlubit Spojené státy (20%), Japonsko (21%) a Lucembursko (21%) (příloha č. 5).

Z hlediska meziročního srovnání, kdy v České republice míra softwarového pirátství klesá, a to z 38% v roce 2008 na 37% v roce 2009, je v sousedním Slovensku míra softwarového pirátství od roku 2008 stagnující, a to 43% (příloha č. 4). V ostatních sousedících zemích má nejvyšší míru pirátství Polsko (54%) s Maďarskem (41%) a nejnižší Rakousko (25%) s Německem. V Rakousku a Německu míra pirátství v roce 2009 vzrostla o jeden procentní bod oproti roku 2008 (příloha č. 3).

Nejvíce se v Česku nelegálně užívají operační systémy Windows, populární kancelářské softwarové balíky, grafické programy, antiviry a počítačové hry. Mezi nejčastěji poškozované výrobce softwaru patří firmy Microsoft, Adobe, Autodesk, Corel a Symantec.

Za posledních patnáct let se v Česku podařilo snížit míru pirátství o 29 procentních bodů (příloha č. 4). Při srovnání s dalšími šestadvaceti členskými státy EU se Česko drží již druhým rokem na jedenácté příčce. Slovensku patří místo šestnácté. V závěsu za

[56] MARTINEZ, Jennifer. *Norton* [online]. 2009 [cit. 2011-01-02]. Ochrana před piráty. Dostupné z WWW: <http://cz.norton.com/products/library/article.jsp?aid=how_to_be_pirate_free>.
[57] *BusinessInfo.cz* [online]. 11.05.2010 [cit. 2011-01-02]. Pirátského softwaru v Česku opět ubylo, nelegálně se ho užívá 37 procent . Dostupné z WWW: <http://www.businessinfo.cz/cz/clanek/kveten-2010/piratskeho-softwaru-v-cesku-opet-ubylo/1001916/57296/>.

Českem jsou mnohé západoevropské a jihoevropské státy, např. Itálie (49%), Španělsko (42%), Francie (40%) (příloha č. 3).

Nejvyšší míru pirátství v rámci EU mají Bulharsko (67%), Rumunsko (65%) a Řecko (58%). Naopak nejnižší mírou pirátství se může pochlubit Lucembursko (21%) a dále Rakousko, Belgie, Finsko, Švédsko a Švýcarsko, které mají 25 % míru pirátství (příloha č. 3).

Ve světě pirátského softwaru v osobních počítačích ubylo. Podle studie BSA a IDC míra pirátství klesla v 54 zemích a vzrostla jen v devatenácti. Přesto celosvětová míra softwarového pirátství vzrostla ze 41 na 43 procent. Došlo k tomu v důsledku, že na globálním softwarovém trhu získaly vyšší podíl rychle se rozvíjející země jako je Indie, Brazílie, Čína, které mají míru pirátství vyšší než ostatní státy. Hodnoty 51,4 miliard amerických dolarů dosáhla v roce 2009 celosvětová komerční hodnota nelegálního softwaru. Nejvyšší celosvětovou míru pirátství, přesahující 90%, mají Gruzie, Zimbabwe a Moldavsko. Naopak nejnižší mírou softwarového pirátství se mohou chlubit již výše zmiňované Spojené státy (20%), Japonsko (21%) a Lucembursko (21%).

V roce 2009 podle IDC připadlo na každých 100 amerických dolarů legálně zakoupeného softwaru dalších 75 dolarů softwaru nelegálního. Pirátství ztenčuje příjmy nejen softwarových firem, ale i státních rozpočtů. Potírání pirátství se proto pozitivně projevuje i v ekonomické rovině. Studie analytiků IDC v roce 2008 poukázala na to, že pokud se sníží míra pirátství o deset procentních bodů, česká ekonomika si během 4 let polepší o tisíce nových pracovních míst, hrubý domácí produkt vzroste o 8,9 miliardy korun a stát na daních vybere téměř dvě miliardy korun. IT firmy se zvýší příjmy o 6,2 miliardy korun a to díky vyšším výdajům za informační technologie. Dále analytici IDC navíc odhadují, že na každý dolar vynaložený za legální krabicový software připadají 3 až 4 dolary příjmů, které jdou do kapsy místním servisním a distribučním firmám – například za instalaci software, školení uživatelů či služby spjaté s údržbou.

Míru pirátství snižují taktéž legalizační programy, osvětové kampaně vládních úřadů i softwarových firem, kroky orgánů činných v trestním řízení a též změny technologií, jako jsou stále rozšířenější nástroje pro správu digitálních práv (DRM) a využívání aplikací usnadňujících hospodaření se softwarem (SAM – Software Asset Management).

Naopak k růstu míry pirátství přispívá rychlý růst trhu s výpočetní technikou a větší užívání starších počítačů, v nichž výskyt nelegálního softwaru převládá. Svou roli hraje i čím dál větší rafinovanost pirátů a kyber-zločinců.[58]

[58] *BusinessInfo.cz* [online]. 11.05.2010 [cit. 2011-01-02]. Pirátského softwaru v Česku opět ubylo, nelegálně se ho užívá 37 procent . Dostupné z WWW: <http://www.businessinfo.cz/cz/clanek/kveten-2010/piratskeho-softwaru-v-cesku-opet-ubylo/1001916/57296/>.

6. ZÁVĚR

Internet a Intranet se neustále rozvíjí. Přináší úžasné kvantum informací potřebných nejen pro osobní potřebu, ale jsou významnými medii zejména v oblasti komunikací.

V diplomové práci byly vymezeny základní rozdíly mezi Internetem a Intranetem, stručně popsána historie a principy fungování, poukázáno na kladné a záporné stránky Internetu a Intranetu, pravidla a zásady slušného chování, které jsou doporučeny dodržovat a portály a projekty zabývající se v současné době bezpečností na Internetu. Celá kapitola byla ukončena dotazníkovým šetřením, kde byly zmapovány vědomosti uživatelů Internetu a Intranetu. Jejich odpovědi byly vyhodnoceny jak slovně, tak pomocí grafů a tabulek. Poté bylo zpracováno vlastní zhodnocení celého výzkumu, příp. navrhnuta doporučení, jak řešit problémy, které uživatelé označili jako nejzávažnější. Šetření dospěla k závěru, že znalost uživatelů zaměřenou na pozitiva, negativa Internetu a Intranetu, internetovou kriminalitu a bezpečnost, je na dobré úrovni.

Další kapitola se zabývala využitelností Internetu a Intranetu Policií ČR. Zde za zmínku stojí, že Policie ČR má na každém oddělení pouze jednu počítačovou sestavu určenou k přístupu do sítě Internet. Intranet mohou využívat všichni policisté a zaměstnanci Policie ČR a je na něj přístup z každého počítače. Internetová stránka zastupující Policii ČR a další složky integrovaného záchranného systému je www.policie.cz. Tato byla mnou rozebrána. V další části byly popsány intranetové stránky Policie ČR, k čemu je policisté a zaměstnanci Policie ČR nejvíce využívají a popsány informační systémy zde se nacházející. Kapitola byla uzavřena dotazníkem zaměřeným na využitelnost internetového portálu www.policie.cz a Intranetu Ministerstva vnitra „HERMES“ v podmínkách Policie ČR. Vytěženo bylo 50 respondentů v rámci Krajského ředitelství policie Karlovarského kraje. Jejich odpovědi byly zpracovány a zjištěno, co by bylo třeba zlepšit či odstranit k zefektivnění jejich práce s návrhy a vlastními doporučeními. U intranetového portálu by bylo vhodné např. zlepšit přehlednost vydáním závazného interního pokynu, nasadit jednotný redakční systém, který umožní vytvořit jednotnou kostru a rozdělí správu určitých okruhů mezi více správců a u internetového portálů PČR např. možnost zdokonalovat tuto webovou stránku obeznámením policistů a zaměstnanců Policie ČR v intranetovém Aplikačním rozcestníku.

Poslední kapitola se týkala softwarové policie, vymezení její činnosti a organizace prosazující práva softwarového odvětví, jako je např. Business Software Alliance, Česká protipirátská unie. Popsána byla softwarová kriminalita, softwarové pirátství, rizika spojená s používáním nelegálního softwaru a ochrana před nimi. Dle údajů uveřejněných organizací BSA bylo provedeno statistické zhodnocení vývoje míry softwarového pirátství v České republice a ostatních světových státech. V České republice se softwarové pirátství snížilo v roce 2009 oproti roku 2008 o jeden procentní bod a Česká republika se tak umístila mezi země s nejnižší mírou softwarového pirátství.

Stanovené cíle byly v diplomové práci naplněny. Celá práce by měla být přínosem jak pro policisty a zaměstnance Policie ČR, tak i širokou veřejnost a začínající uživatele. Tito by si po jejím přečtení měli uvědomit, co jim všechno Internet a Intranet nabízí a čeho by se měli při práci v těchto sítích vyvarovat. Práce byla obohacena o různé názory, které zde byly zapracovány.

7. SEZNAM POUŽITÝCH ZDROJŮ

1. *Datacentrum WEDOS* [online].WEDOS Internet, a.s., 26.01.2010 [cit. 2010-10-24]. Co je Internet a jak funguje?. Dostupné z WWW: <http://datacentrum.wedos.com/a/17/co-je-internet-jak-funguje.html>.
2. *SeniorClub* [online]. 2007 [cit. 2010-10-24]. HISTORIE INTERNETU. Dostupné z WWW: <http://www.seniorclub.cz/internet.htm>.
3. *PragueBest* [online]. 2010 [cit. 2010-10-24]. Firemní intranet. Dostupné z WWW: <http://www.praguebest.cz/firemni-intranet.html>.
4. ČERMÁK, Miloš. *Internet snadno a rychle : Na Internetu jako doma v devíti krátkých kapitolách*. Praha : Moraviapress,a.s., 2002. 43 s.
5. *Radim Chlad (xchlad@fi.muni.cz)* [online]. 2000 [cit. 2010-10-24]. Historie Internetu v České republice. Dostupné z WWW: <http://www.fi.muni.cz/usr/jkucera/pv109/2000/xchlad.htm>.
6. *EXTRA.NET* [online]. 2007 [cit. 2010-10-24]. Historie Intranetu. Dostupné z WWW: <http://i-extra.net/it/internet-a-site/historie-internetu/>.
7. *Referáty-seminárky.cz* [online]. Universita Pardubice : 2007 [cit. 2010-10-24]. Intranet. Dostupné z WWW: <http://referaty-seminarky.cz/intranet/>. ISSN 1802-422X.
8. NOVÁK, Josef; VLADIMÍR, Ludva; DVORSKÝ, Jakub. *@beceda internetu*. Vyd. 1. Praha : Computer press , 2000. 78 s. ISBN 8072263692.
9. *Wikipedie : Otevřená encyklopedie* [online]. 2009, poslední změna: 29. 8. 2010 v 10:26. [cit. 2010-10-24]. Intranet. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Intranet>.
10. *Český statistický úřad* [online]. Praha : 2009, poslední změna: 12.8. 2010 [cit. 2010-10-24]. Internet a komunikace. Dostupné z WWW: <http://www.czso.cz/csu/redakce.nsf/i/internet_a_komunikace>.
11. KRŠKOVÁ, Milena; PLEVA, Radovan. *Širokopásmové sítě a jejich aplikace : Moderní komunikační technologie datových a počítačových sítí a jejich aplikace, internet/intranet, WWW, videokonference*. Olomouc : Poligrafické středisko VUP, 2000. 113 s. ISBN 80-244-0095-2.

12. PRAVDOVÁ, Eliška; JEŽKOVÁ, Zuzana. *Máma a já* [online]. 22.07.2009 [cit. 2011-01-02]. Jak se chytí láska v síti. Dostupné z WWW: <http://www.mamaaja.cz/ActiveWeb/Article/1496/jak_se_chyti_laska_v.html>.
13. NOVÁKOVÁ, Daniela. *Měšec.cz* [online]. 2. 7. 2003 [cit. 2011-01-02]. Nakupujte přes Internet!. Dostupné z WWW: <http://www.mesec.cz/clanky/nakupujte-pres-internet/>. ISSN 1213-4414.
14. *Bezpečí* [online]. 2008, poslední změna: 5.6. 2008 [cit. 2010-10-24]. Internet a kyberšikana . Dostupné z WWW: <http://cms.e-bezpeci.cz/content/view/36/63/lang,czech/>.
15. *IReferáty.cz* [online]. 2005 [cit. 2010-10-24]. Internet. Dostupné z WWW: <http://ireferaty.lidovky.cz/309/1208/Internet>.
16. *IDNES.cz : Finance* [online]. 2005 [cit. 2010-10-24]. Co všechno umí internetové bankovnictví. Dostupné z WWW: <http://finance.idnes.cz/viteze.asp?r=viteze&c=A050427_162054_viteze_zal>.
17. *FG Forrest* [online]. 2009 [cit. 2010-10-24]. Intranety. Dostupné z WWW: <http://www.fg.cz/cs/nabidka/webova-reseni/intranety.shtml>.
18. *Ústřední knihovna ČVUT* [online]. 2006, poslední změna: 12. 3. 2007 [cit. 2010-10-24]. Další informační zdroje na Internetu. Dostupné z WWW: <http://platan.vc.cvut.cz/vychova/vyuka-fs/zdroje.html>.
19. KACHLÍK, Petr. *Pedagogická fakulta Masarykovy univerzity v Brně : katedra speciální pedagogiky* [online]. 2005 [cit. 2011-01-02]. Handicapovaní a Internet . Dostupné z WWW: <http://natura.baf.cz/natura/2003/2/20030205.html>.
20. *@Bezpečný internet.cz* [online]. 2009 [cit. 2010-10-24]. Spam. Dostupné z WWW: <http://www.bezpecnyinternet.cz/zacatecnik/e-mail/spam.aspx>.
21. *Microsoft* [online]. 2009 [cit. 2010-10-24]. Co je počítačový virus?. Dostupné z WWW: <http://www.microsoft.com/cze/athome/security/viruses/intro_viruses_what.mspx>.
22. PAUKERTOVÁ, Veronika. *IKAROS* [online]. 2006 [cit. 2010-10-24]. Elektronická informační kriminalita. Dostupné z WWW: <http://www.ikaros.cz/elektronicka-informacni-kriminalita#l5>. ISSN 1212-5075.

23. *Digitálně.cz : Magazín stahuj* [online]. 2009 [cit. 2010-10-24]. Jak porno změnilo internet? 1. díl. Dostupné z WWW: <http://digitalne.centrum.cz/jak-porno-zmenilo-internet-1-dil/>.
24. *Safer : Internet.cz* [online]. 2010 [cit. 2010-10-24]. Za bezpečné prostředí virtuálního světa. Dostupné z WWW: <http://www.saferinternet.cz/>.
25. CIBULKA, Karel. *IPrávník* [online]. 2009 [cit. 2010-10-24]. K trestným činům spáchaným při protiprávním nakládání s léčivy. Dostupné z WWW: <http://www.ipravnik.cz/cz/clanky/art_6561/k-trestnym-cinum-spachanym-pri-protipravnim-nakladani-s-lecivy.aspx>.
26. PROTIVÍNSKÝ, Miroslav. Internetová kriminalita : (Z německých zkušeností). In *Kriminalistika : čtvrtletník pro kriminalistickou teorii a praxi.* 2. vyd. [s.l.] : [s.n.], 2002. s. 1. Dostupný z WWW: <http://www.mvcr.cz/casopisy/kriminalistika/2002/02_02/protivin.html>.
27. *HOAX.cz* [online]. 2008 [cit. 2010-10-24]. Co je to phishing. Dostupné z WWW: <http://hoax.cz/phishing/co-je-to-phishing>.
28. JIROVSKÝ, Václav; HNÍK, Václav; KRULÍK, Oldřich. *MVCR.cz* [online]. 2005 [cit. 2010-10-24]. ZÁKLADNÍ DEFINICE, VZTAHUJÍCÍ SE K TÉMATU KYBERNETICKÝCH HROZEB. Dostupné z WWW: <http://aplikace.mvcr.cz/archiv2008/bezpecnost/informacni/zakladni_info.pdf>.
29. JIROVSKÝ, Václav, et al. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* . Vyd. 1. Praha : Grada, 2007. 287 s. ISBN 978-80-247-1561-2.
30. HYNEK, J. *Intranet není jen o dokumentech : Moderní řízení*. č.10. Praha : Economia, 2003. 48 s.
31. PETERKA, Jiří. *EArchiv.cz* [online]. 2008 [cit. 2010-10-24]. Netiquette. Dostupné z WWW: <http://www.earchiv.cz/axxxk160/a705k164.php3>.
32. *Bezpečně-online.cz* [online]. 2010 [cit. 2010-10-24]. Etiketa, netiketa, chatiketa. Dostupné z WWW: <http://www.bezpecne-online.cz/surfuj-bezpecne/komunikace-se-svetem/etiketa-netiketa-chatiketa/205-3/netiketa>.
33. Česko. Využívání datové sítě Intranet Ministerstva vnitra „HERMES". In *Závazný pokyn policejního prezidenta*. 9.8. 2005, 2005, 72, 80, s. 14.

34. *Horkálinka.cz : Bojujeme proti internetové kriminalitě* [online]. 2009 [cit. 2010-10-24]. Horká linka. Dostupné z WWW: <http://horka-linka.saferinternet.cz/>.
35. *Sdružení Linka bezpečí* [online]. 2009 [cit. 2010-10-24]. Telefonická pomoc dětem. Dostupné z WWW: <http://www.linkabezpeci.cz/webmagazine/home.asp?idk=393>.
36. *Protišikaně.cz* [online]. 2009 [cit. 2010-10-24]. KAMPAŇ PROTI ŠIKANĚ. Dostupné z WWW: <http://proti-sikane.saferinternet.cz/>.
37. *Safer : Internet.cz* [online]. 2009 [cit. 2010-10-24]. O projektu. Dostupné z WWW: <http://www.saferinternet.cz/o-projektu/538-3>.
38. *EBezpečí.cz* [online]. 2008 [cit. 2010-10-24]. Bezpečný internet. Dostupné z WWW: <http://www.ebezpeci.cz/projekt.php>.
39. *@Bezpečný internet.cz* [online]. 2009 [cit. 2010-10-24]. O projektu. Dostupné z WWW: <http://www.bezpecnyinternet.cz/o-projektu/default.aspx>.
40. *Policie.cz : Policie České republiky – KŘP Moravskoslezského kraje* [online]. 2010 [cit. 2010-10-24]. (NE)bezpečný Internet. Dostupné z WWW: <http://www.policie.cz/clanek/ne-bezpecny-internet.aspx>.
41. RAK, Roman, et al. *Informatika v kriminalistické a bezpečnostní praxi* [online]. Správa Zpč. kraje Plzeň : Odbor spojení a informatiky MV ČR, 2009 [cit. 2011-01-02]. Dostupné z WWW: <http://kszc-app.ks.zc/oikt/index.html>.
42. *Policejní prezidium* [online]. 2009 [cit. 2011-01-02]. Schengenský informační systém – SIS. Dostupné z WWW: <http://mail-inter.pcr.cz/interpol/Sierene/SIS.htm>.
43. *Praha OSŘI* [online]. 2009 [cit. 2011-01-02]. Informační systémy. Dostupné z WWW: <http://cportal.pcr.cz/inf_sys/prospekty/default.asp>.
44. AMBROŽ, Jan. *LUPA.cz* [online]. 24. 5. 2005 6:30 [cit. 2011-01-02]. Jak silná je naše "softwarová policie"?. Dostupné z WWW: <http://www.lupa.cz/clanky/jak-silna-je-nase-softwarova-policie/>.
45. *BSA* [online]. 2009 [cit. 2011-01-02]. Co je softwarové pirátství?. Dostupné z WWW: <http://www.bsa.org/country.aspx?sc_lang=cs-CZ>.
46. *Česká protipirácká unie* [online]. 2009 [cit. 2011-01-02]. Kdo jsme a čím se zabýváme. Dostupné z WWW: <http://www.cpufilm.cz/kdo_jsme.html>.
47. *Microsoft* [online]. 2009 [cit. 2011-01-02]. Čtyři nejběžnější typy softwarové kriminality. Dostupné z WWW: <Čtyři nejběžnější typy softwarové kriminality>.

48. *Bezpečný internet.cz* [online]. 2009 [cit. 2011-01-02]. Rizika používání nelegálních programů - softwarové pirátství. Dostupné z WWW: <http://www.bezpecnyinternet.cz/pokrocily/stahovani-souboru-programu/softwarove-piratstvi.aspx>.
49. MARTINEZ, Jennifer. *Norton* [online]. 2009 [cit. 2011-01-02]. Ochrana před piráty. Dostupné z WWW: <http://cz.norton.com/products/library/article.jsp?aid=how_to_be_pirate_free>.
50. *BusinessInfo.cz* [online]. 11.05.2010 [cit. 2011-01-02]. Pirátského softwaru v Česku opět ubylo, nelegálně se ho užívá 37 procent . Dostupné z WWW: <http://www.businessinfo.cz/cz/clanek/kveten-2010/piratskeho-softwaru-v-cesku-opet-ubylo/1001916/57296/>.

8. PŘÍLOHY

1. Dotazník na téma „Klady a zápory Internetu a Intranetu, internetová kriminalita a bezpečnost“
2. Dotazník na téma „Využitelnost Internetu a Intranetu Policií ČR“
3. Míra pirátství v jednotlivých státech EU v r. 2009
4. Vývoj míry softwarového pirátství v Česku a na Slovensku (1994 – 2009)
5. Země s nejnižší a nejvyšší mírou softwarového pirátství v roce 2009

Příloha č. 1

Dotazník na téma „Klady a zápory Internetu a Intranetu, internetová kriminalita a bezpečnost“

Dotazník na výše uvedené téma slouží ke zmapování situace, zda si běžní uživatelé Internetu a podnikového Intranetu uvědomují, jaká pozitiva či negativa mohou tyto dvě sítě přinášet, s tím spojenou internetovou kriminalitu a bezpečnostní pravidla, která je vhodné dodržovat.

Dotazník je anonymní. Jednu vyhovující odpověď prosím zakroužkujte, případně doplňte slovní odpověď.

1. Jste:

a) muž **b)** žena

2. V jaké věkové kategorii se pohybujete?

a) méně než 30 **b)** 31 - 40 **c)** 41 - 50 **d)** 51 a více

3. Jaké je Vaše vzdělání?

a) ÚSO **b)** SŠ **c)** VOŠ **d)** VŠ

4. Je pro Vás Internet a Intranet důležitý k životu?

Internet:

a) ano
b) spíše ano
c) spíše ne
d) ne

Intranet:

a) ano
b) spíše ano
c) spíše ne
d) ne

5. Jak dlouho používáte Internet a jak dlouho Intranet?

Internet:

a) méně než 1 rok
b) 1 – 2 roky
c) 2 – 5 let
d) 5 – 10 let
e) 10 – a více
f) vůbec ho nepoužívám

Intranet:

a) méně než 1 rok
b) 1 – 2 roky
c) 2 – 5 let
d) 5 – 10 let
e) 10 – a více
f) vůbec ho nepoužívám

6. Kolik hodin denně strávíte na Internetu a kolik na Intranetu?

Internet:	*Intranet:*
a) méně jak 1 hodinu denně	**a)** méně jak 1 hodinu denně
b) 1 – 3 hodiny denně	**b)** 1 – 3 hodiny denně
c) 3 – 6 hodin denně	**c)** 3 – 6 hodin denně
d) 6 a více hodin denně	**d)** 6 a více hodin denně
e) žádná z nabízených variant	**e)** žádná z nabízených variant

7. Co nejvíce využíváte prostřednictvím Internetu a Intranetu? Uveďte 3 příklady.

Internet:	*Intranet:*
1. …….	…….
2. ……..	……..
3. ……..	……..

8. Jaké kladné stránky si myslíte, že přináší Internet a jaké Intranet? Uveďte 3 příklady.

Internet:	*Intranet:*
1. …….	…….
2. ……..	……..
3. ……..	……..

9. Jaké záporné stránky spatřujete v Internetu a jaké v Intranetu? Uveďte 3 příklady.

Internet:	*Intranet:*
1. …….	…….
2. ……..	……..
3. ……..	……..

10. Jaký způsob komunikace využíváte nejvíce na Internetu?

a) e-mail
b) telefonování
c) ostatní (např. chat, videokonference atd.)
d) žádný

a jaký na Intranetu?

a) e-mail
b) diskusní fórum
c) chat
d) nevyužívám žádný
e) jiný, než shora uvedené množnosti (uveďte jaký) **……..**

11. Pracujete pomocí Internetu s choulostivými daty (např. internetové bankovnictví, intimní fotky, burzovní obchody atd.)?

a) ano, velmi často, důvěřuji všem
b) ano, velmi často, ale vždy s maximální opatrností
c) pouze v nejnutnějších případech
d) ne, nikdy bych přes Internet neposílal choulostivá data

12. Bojíte se, že byste se mohli stát terčem nebo účastníkem internetové kriminality?

a) ano **b)** spíše ano **c)** spíše ne **d)** ne

13. Stali jste se již někdy terčem nebo se Vám naskytla možnost se stát účastníkem z některých následujících událostí?

a) vydírání, výhružky, urážky
b) spam
c) phishing
d) poškození či odcizení soukromých dat
e) nic z výše uvedeného

14. Z internetových trestných činů se Vám jeví jako nejhorší?

a) šíření pornografie
b) porušování autorského práva
c) kyberšikana
d) internetové podvody (např. phishing, pharming, sociální inženýrství)
e) jiný (uveďte jaký) **…….**

15. Jakým způsobem si opatřujete např. software, filmy, hudbu?

a) kupuji je
b) pomocí P2P sítí (např. Torrenty)
c) od přátel, známých
d) stahuji je zdarma z volně dostupných internetových stránek (freehostingové služby)

16. Jak byste postupně ohodnotili od 1 - 6 rizika spojená s používáním nelegálního softwaru? (1 – nejvíce závažná, 6 nejméně závažná)

RIZIKA :	1	2	3	4	5	6
Trestní postih za používání nelegálního softwaru						
Ztráta dat						
Virové nákazy počítače						
Finanční ztráta						
Ztráta soukromí						
Nemožnost aplikovat bezpečnost a funkční aktualizaci						

A jakou považujete nejdůležitější ochranu, abyste rizikům předcházeli?

a) zakoupení softwaru od autorizovaného prodejce
b) zkontrolovat adresu URL webové stránky před poskytnutím informací o kreditní kartě
c) při nákupu online zkontrolovat, zda web je pravý pomocí certifikátu zabezpečení
d) ani jedna z nabízených možností není vyhovující

17. Pokud byste chtěli navštívit některé stránky, které nabízejí např. pornografii, xenofobii, rasismus apod., myslíte si, že byste je dokázali najít?

a) ano **b)** spíše ano **c)** spíše ne **d)** ne

18. Jaká zásada slušného chování na Internetu a na Intranetu je pro Vás nejdůležitější, kterou by měl každý člověk dodržovat?
Ohodnoťte postupně od 1-4, kdy 1 je nejdůležitější a 4 nejméně důležitá.

Internet:

a) nepoužívat počítač ke škodě jiného **…….**
b) nezasahovat do práce druhých lidí **…….**
c) nepoužívat počítač pro křivé svědectví **…….**
d) nepoužívat počítač ke krádeži **…….**

Intranet:

a) po skončení práce na pracovní stanici provést odhlášení a pracovní stanici vypnout nebo ji zajistit proti neoprávněnému použití **…….**
b) informovat administrátora lokální sítě o skutečnosti, které by mohla způsobit ohrožení bezpečnosti nebo funkčnosti sítě Intranet, a o zjištění poruchy některé služby sítě Intranet **…….**
c) nepřipojovat jiné počítačové sestavy, než které byly připojeny administrátorem **…….**
d) neumožnit ostatním pracovníkům použít mé uživatelské konto při práci v síti Intranet **…….**

19. Ohodnoťte postupně od 1-3, kdy 1 je nejlepší, 3 nejhorší, který z projektů zabývající se bezpečností Internetu se Vám jeví jako nejlepší? Pokud jsou Vám tyto projekty neznámí, zakroužkujte za d).

a) Safer Internet (Bezpečný Internet) **…….**
b) E-bezpečí **…….**
c) Bezpečný internet.cz **…….**
d) žádný z výše uvedených neznám

20. Jaké využíváte programy na zabezpečení?

a) freeware (zdarma)
b) profesionální komerční programy
c) nástroje integrované v systému např. Microsoft firewall
d) jiné

Příloha č. 2

Dotazník na téma „Využitelnost internetového portálu PČR (www.policie.cz) a Intranetu Ministerstva vnitra „HERMES“ v podmínkách Policie ČR“

Tento dotazník je určen pro policisty a civilní pracovníky Policie ČR. Zaměřuje se na výzkum, zda a jak policisté a zaměstnanci Policie ČR využívají pro výkon své služby/práce internetový portál www.policie.cz a Intranet Ministerstva vnitra „HERMES“ v podmínkách PČR.

Dotazník je anonymní. Jednu vhodnou odpověď prosím zakroužkujte, popř. doplňte slovní odpověď.

1. Jste:

a) muž **b)** žena

2. V jaké věkové kategorii se pohybujete?

a) méně než 30 **b)** 31 - 40 **c)** 41 - 50 **d)** 51 a více

3. Jaké je Vaše vzdělání?

a) ÚSO **b)** SŠ **c)** VOŠ **d)** VŠ

4. Jaké je Vaše pracovní zařazení?

a) vedoucí pracovník **b)** policista **c)** administrativní pracovník

d) zaměstnanec údržby **e)** jiné než z nabízených možností

5. Využíváte při výkonu své služby/práce WWW server Policie ČR?

a) ano **b)** spíše ano **c)** spíše ne **d)** ne

Využíváte při výkonu své služby/práce Intranet?

a) ano **b)** spíše ano **c)** spíše ne **d)** ne

6. Kolik času strávíte denně na internetovém a kolik na intranetovém portále PČR?

Internet:	*Intranet:*
a) méně jak 1 hodinu denně	**a)** méně jak 1 hodinu denně
b) 1-2 hodiny denně	**b)** 1-2 hodiny denně
c) 2 a více hodin denně	**c)** 2 a více hodin denně
d) žádný čas (0 hodin)	**d)** žádný čas (0 hodin)

7. Co nejčastěji využíváte na internetových stránkách PČR (www.policie.cz) a co na Intranetu PČR? Uveďte 3 příklady.

Internet:	*Intranet:*
1. …….	…….
2. ……..	……..
3. ……..	……..

8. Jsou informace na internetových stránkách www.policie.cz a na intranetových stránkách PČR aktuální a přehledné?

***Internetové stránky www.policie.cz**:*

a) ano **b)** spíše ano **c)** spíše ne **d)** ne

Intranetové stránky PČR:

a) ano **b)** spíše ano **c)** spíše ne **d)** ne

9. Existuje dobrá provázanost mezi jednotlivými resorty Policie ČR pomoci Internetu?

a) ano **b)** spíše ano **c)** spíše ne **d)** ne

Existuje dobrá provázanost mezi jednotlivými resorty Policie ČR pomoci Intranetu?

a) ano **b)** spíše ano **c)** spíše ne **d)** ne

10. Využíváte při své práci databázové systémy z internetových stránek www.policie.cz?

a) ano **b)** spíše ano **c)** spíše ne **d**) ne

V případě odpovědí za a) a b) uveďte, jaké 3 databázové systémy nejvíce využíváte.

Odpověď: **1.)** …….

2.) …….

3.) …….

Využíváte při své práci informační systémy z intranetových stránek PČR?

a) ano **b)** spíše ano **c)** spíše ne **d)** ne

V případě odpovědi za a) a b) uveďte, jaké 3 informační systémy nejvíce využíváte.

Odpověď: **1.)** …….

2.) …….

3.) …….

11. Sledujete pravidelně informace zveřejňované na internetovém portálu www.policie.cz a na policejních intranetových stránkách?

Internetový portál www.policie.cz:

a) ano **b)** spíše ano **c)** spíše ne **d)** ne

Policejní intranetové stránky:

a) ano **b)** spíše ano **c)** spíše ne **d)** ne

Jak často takto zveřejňované informace sledujete?

Internetový portál www.policie.cz:

a) velmi často (několikrát denně)
b) často (1x – 2x týdně)
c) méně často (1x – 2x měsíčně)
d) pouze, pokud jsem k tomu upozorněn/a mým vedoucím
e) nikdy

Policejní intranetové stránky:

a) velmi často (několikrát denně)
b) často (1x – 2x týdně)
c) méně často (1x – 2x měsíčně)
d) pouze, pokud jsem k tomu upozorněn/a mým vedoucím
e) nikdy

12. Dodržujete bezpečnostní zásady spojené s užíváním sítě internetového portálu www.policie.cz a Intranetu PČR?

Internetový portál www.policie.cz:
a) ano **b)** spíše ano **c)** spíše ne **d)** ne

Intranet PČR:
a) ano **b)** spíše ano **c)** spíše ne **d)** ne

V případě odpovědi za a) a b) uveďte jaké? (max. 3)

……

……

……

V případě odpovědi za c) a d) uveďte proč?

……

……

……

13. Můžete sami navrhovat změny nebo zasílat nápady na zlepšení funkcí internetových a intranetových stránek PČR?

Internet:

a) ano, mohu a činím tak
b) ano, mohu, ale nečiním tak
c) ne, nemohu, ale rád/a bych
d) ne, nemohu a nechci
e) nevím

Intranet:

a) ano, mohu a činím tak
b) ano, mohu, ale nečiním tak
c) ne, nemohu, ale rád/a bych
d) ne, nemohu a nechci
e) nevím

14. Co byste zlepšili na internetových a intranetových stránkách PČR? Uveďte 3 příklady.

Internet (www.policie.cz):	*Intranet:*
1. ……	……
2. ……	……
3. ……	……

15. Co byste naopak z internetových a intranetových stránek PČR odstranili? Uveďte 3 příklady.

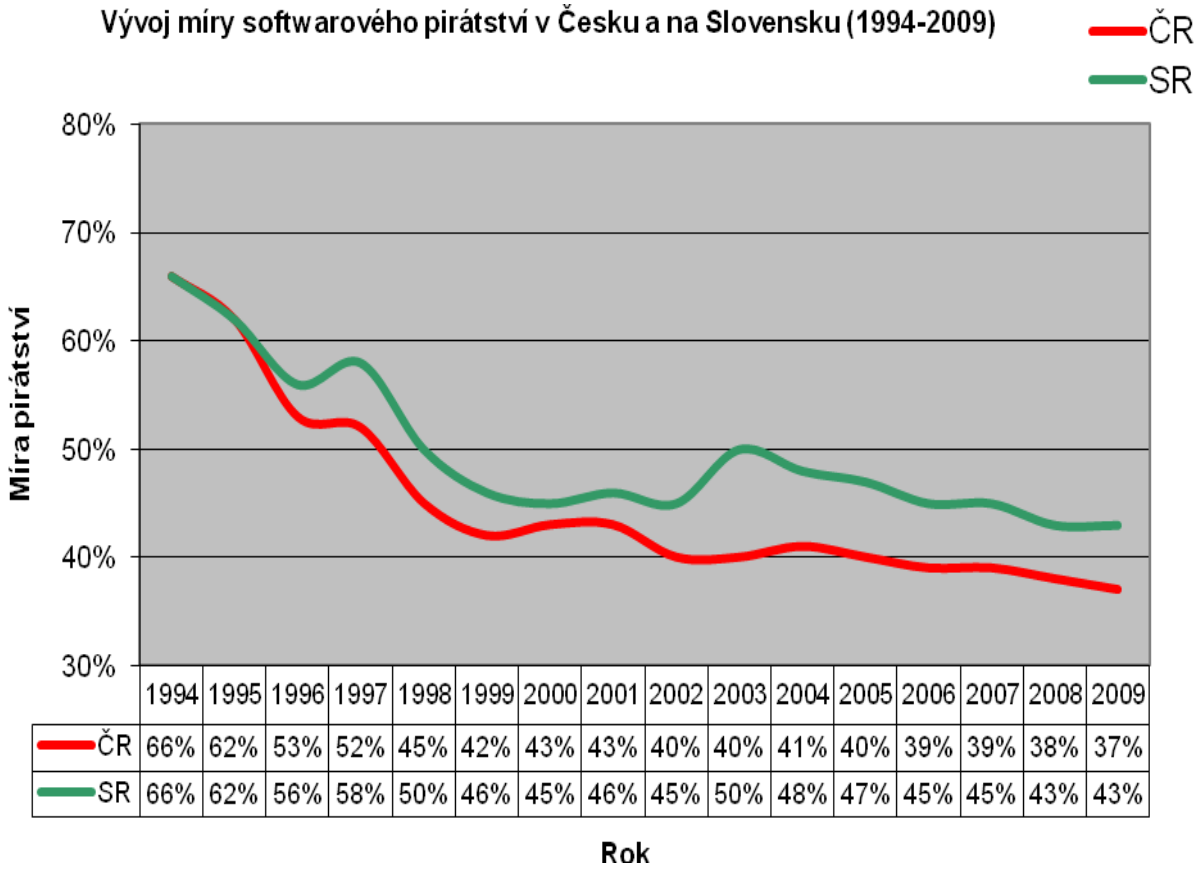
Internet (www.policie.cz):	*Intranet:*
1. ……	……
2. ……	……
3. ……	……

Míra pirátství v jednotlivých státech Evropské unie v roce 2009

			MÍRA PIRÁTSTVÍ					ZTRÁTY V MIL. USD	
pořadí	**země**	**rozdíl**	**2009**	**2008**	**2007**	**2006**	**2005**	**2009**	**$M**
1.	Lucembursko	**0%**	**21%**	21%	21%			**$**	**30**
2.	Rakousko	**1%**	**25%**	24%	25%	26%	26%	**$**	**212**
3.	Belgie	**0%**	**25%**	25%	25%	27%	28%	**$**	**239**
4.	Finsko	**-1%**	**25%**	26%	25%	27%	26%	**$**	**175**
5.	Švédsko	**0%**	**25%**	25%	25%	26%	27%	**$**	**304**
6.	Dánsko	**1%**	**26%**	25%	25%	25%	27%	**$**	**203**
7.	Velká Británie	**0%**	**27%**	27%	26%	27%	27%	**$**	**1581**
8.	Německo	**1%**	**28%**	27%	27%	28%	27%	**$**	**2023**
9.	Nizozemsko	**0%**	**28%**	28%	28%	29%	30%	**$**	**525**
10.	Irsko	**1%**	**35%**	34%	34%	36%	37%	**$**	**125**
11.	Česká rep.	**-1%**	**37%**	38%	39%	39%	40%	**$**	**174**
12.	Francie	**-1%**	**40%**	41%	42%	45%	47%	**$**	**2544**
13.	Portugalsko	**-2%**	**40%**	42%	43%	43%	43%	**$**	**221**
14.	Maďarsko	**-1%**	**41%**	42%	42%	42%	42%	**$**	**113**
15.	Španělsko	**0%**	**42%**	42%	43%	46%	46%	**$**	**1014**
16.	Slovensko	**0%**	**43%**	43%	45%	45%	47%	**$**	**65**
17.	Malta	**0%**	**45%**	45%	46%	45%	45%	**$**	**7**
18.	Slovinsko	**-1%**	**46%**	47%	48%	48%	50%	**$**	**39**
19.	Kypr	**-2%**	**48%**	50%	50%	52%	52%	**$**	**16**
20.	Itálie	**1%**	**49%**	48%	49%	51%	53%	**$**	**1733**
21.	Estonsko	**0%**	**50%**	50%	51%	52%	54%	**$**	**19**
22.	Litva	**0%**	**54%**	54%	56%	57%	57%	**$**	**31**
23.	Polsko	**-2%**	**54%**	56%	57%	57%	58%	**$**	**506**
24.	Lotyšsko	**0%**	**56%**	56%	56%	56%	57%	**$**	**24**
25.	Řecko	**1%**	**58%**	57%	58%	61%	64%	**$**	**248**
26.	Rumunsko	**-1%**	**65%**	66%	68%	69%	72%	**$**	**183**
27.	Bulharsko	**-1%**	**67%**	68%	68%	69%	71%	**$**	**115**
	Evropská unie		**35%**	35%	35%	36%	36%	**$**	**12 469**

zdroj: BSA

Příloha č. 4



	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009
ČR	66%	62%	53%	52%	45%	42%	43%	43%	40%	40%	41%	40%	39%	39%	38%	37%
SR	66%	62%	56%	58%	50%	46%	45%	46%	45%	50%	48%	47%	45%	45%	43%	43%

zdroj: BSA

Příloha č. 5

Země s nejnižší a nejvyšší mírou softwarového pirátství v roce 2009

země s nejvyšší mírou softwarového pirátství		
pořadí	**země**	**2009**
1.	Gruzie	95 %
2.	Zimbabwe	92 %
3.	Bangladéš	91 %
	Moldavsko	91 %
4.	Arménie	90 %
	Jemen	90 %
5.	Srí Lanka	89 %
6.	Ázerbájdžán	88 %
	Libye	88 %
7.	Bělorusko	87 %
	Venezuela	87 %
8.	Indonésie	86 %
9.	Irák	85 %
	Ukrajina	85 %
	Vietnam	85 %
10.	Alžírsko	84 %
	Pákistán	84 %
11.	Kamerun	83 %
	Nigérie	83 %
12.	Paraguay	82 %
	Zambie	82 %
13.	Černá Hora	81 %
14.	Bolívie	80 %
	Salvador	80 %
	Guatemala	80 %
15.	Botswana	79 %
	Čína	79 %
	Pobřeží slonoviny	79 %
	Keňa	79 %
	Nikaragua	79 %

země s nejnižší mírou softwarového pirátství		
pořadí	**země**	**2009**
1.	USA	20
2.	Japonsko	21
	Lucembursko	21
4.	Nový Zéland	22
5.	Austrálie	25
	Rakousko	25
	Belgie	25
	Finsko	25
	Švédsko	25
	Švýcarsko	25
6.	Dánsko	26
7.	Velká Británie	27
8.	Německo	28
	Nizozemsko	28
9.	Kanada	29
	Norsko	29
10.	Izrael	33
11.	Irsko	35
	Singapur	35
	Jihoafrická republika	35
12.	Spojené arabské	36
13.	Česká republika	37
14.	Tchaj-wan	38
15.	Francie	40
	Portugalsko	40
	Réunion	40
16.	Maďarsko	41
	Jižní Korea	41
17.	Španělsko	42
18.	Slovensko	43

zdroj: BSA