Základní pojmy a bezpečnost

Základní pojmy

Internet je decentralizovaná rozsáhlá síť spojující počítače a jiné sítě (počítače v nich komunikují pomocí rodiny protokolů TCP/IP) na celém světě. Pokud připojíme počítač do sítě Internet, tak získáme přístup ke službám, které Internet poskytuje. Nejpoužívanější službou Internetu je **World Wide Web.**

WWW (World Wide Web) je celosvětová soustava vzájemně propojených dokumentů. Dokumenty umístěné na počítačových serverech jsou adresovány pomocí **URL (Uniform Resource Locator).**

URL je synonymem pro internetové adresy. Jedná se o způsob, jak jednoznačně zapsat umístnění souboru na Internetu nebo intranetu. Pro přístup na internetové stránky musíme znát URL adresu, která má většinou následující tvar: **http://www.uzlabina.cz**. První část internetové adresy tvoří přenosový protokol **(http)**, další část je tvořena doménovým jménem, které se skládá z domény třetího řádu **(www)**, doménou druhého řádu **(uzlabina)** a domény prvního (nejvyššího) řádu **(cz).**

Doménové jméno je tvořeno posloupností několika částí oddělenými tečkami. Tyto části jsou seřazeny podle obecnosti: doména 3. řádu, doména 2. řádu, doména 1. řádu. **Domény prvního (nejvyššího) řádu** členíme na domény **národní** a domény **organizací.** Národní domény jsou tvořeny dvěma znaky (např.: .cz, .sk, .uk, .us). Mezi známé domény organizací patří například: .com, .edu, .info, .net, .org.

Hypertextový odkaz je základním prvkem hypertextových dokumentů. Takový odkaz může odkazovat jak na celý dokument, tak i na specifické části dokumentu. Pomocí hypertextového odkazu také přecházíme na jinou webovou stránku, která může být umístěná na jiném počítači.

Pro zobrazení dokumentů vytvořených prostřednictvím jazyka **HTML** (HyperText Markup Language) slouží programy, které nazýváme **internetové prohlížeče.** Mezi nejpoužívanější prohlížeče patří **Internet Explorer, Mozilla Firefox, Google Chrome, Safari** a **Opera.**





Na internetu můžeme realizovat různé aktivity, např.:

- vyhledávání informací,
- nakupování,
- vzdálená výuka (e-learning) – jedná se o využití výpočetní techniky k tvorbě vzdělávacích materiálů v elektronické podobě a používání sítě Internet k distribuci studijního obsahu, k řízení studia a ke komunikaci mezi studenty a pedagogy,
- publikování informací,
- používání elektronického bankovnictví,
- využívání služeb státní správy – výkon veřejné správy s využitím ICT (např. Czech POINT, Datové schránky, Portál veřejné správy),
- zábava a komunikace.

Bezpečnost a zabezpečení

Při používání Internetu je důležité znát a dodržovat **základní pravidla bezpečnosti.** Mezi hlavní zásady bezpečnosti patří:

- nesdělování osobních a finančních informací,
- nakupování na zabezpečených internetových stránkách důvěryhodných prodejců,
- odhlašování od internetových stránek po ukončení nebo při přerušení práce.

Pro bezpečnější komunikaci mezi uživatelem a konkrétní webovou stránkou (např. elektronické bankovnictví) se komunikace zašifruje na základě zabezpečeného protokolu **HTTPS** (HyperText Transfer Protocol Secured). Takto zabezpečenou internetovou stránku můžeme rozpoznat **podle protokolu** nebo podle **symbolu zámku**, který se zobrazí v adresním řádku internetového prohlížeče. Ukázku zabezpečené internetové stránky vidíme na obrázcích (postupně zobrazeno v prohlížeči Google Chrome, Internet Explorer, Mozilla Firefox).

Šifrování dat je proces, kterým se nezabezpečená elektronická data převádí za pomoci kryptografie na data šifrovaná, čitelná pouze pro majitele dešifrovacího klíče. Šifrování dat slouží k jejich ochraně proti nežádoucímu zjištění cizí osobou a uplatňuje se při ukládání dat i při jejich přenosu včetně telekomunikace.

U zabezpečených internetových stránek si může uživatel zobrazit tzv. **digitální certifikát.** Digitální certifikát je soubor dat, který identifikuje osobu nebo server a může během komunikace mezi dvěma subjekty zajistit šifrování přenášených dat. Certifikáty jsou používány pro identifikaci protistrany při vytváření zabezpečeného spojení. Digitální certifikáty vystavuje **certifikační autorita.** V České republice fungují tyto certifikační autority: První certifikační autorita, a. s., Česká pošta, s. p., eldentity a. s.

Podrobnosti o digitálním certifikátu může uživatel zobrazit prostřednictvím internetového prohlížeče. Většinou stačí poklepat na symbol zámku v adresním řádku prohlížeče (viz ukázka).

Využívání Internetu má pro některé uživatele i svá **omezení** (např. dohled, omezení prohlížených webových stránek, omezení stahování dat).

Informace z Internetu

Vyhledávání

Internetový vyhledávač je program, který uživateli umožňuje prohledávání Internetu podle zadaných kritérií. Internetové vyhledávače se dělí na fulltextové a katalogové.

Fulltextové vyhledávače jsou programy, které vyhledávají v celém textu. Takový vyhledávač hledá po Internetu webové stránky, dokumenty (textové, pdf, obrázky), které indexuje do své vlastní databáze a následně umožňuje pomocí jednoduchých či složitých dotazů přístup do této databáze a vypisuje odkazy na jednotlivé dokumenty. Nejznámější fulltextový vyhledávač je Google.

Katalogové vyhledávače obsahují odkazy na jiné webové stránky a portály. Odkazy jsou tematicky setříděny, může se procházet jednotlivými sekcemi nebo i vyhledávat podle jednoduchých dotazů. Záznam do katalogu se provádí registrací do příslušné sekce. Mezi neznámější české a zahraniční katalogové vyhledávače patří: Seznam, Centrum, Atlas, Yahoo.

Kritické zhodnocení obsahu

Pro uživatele je velmi důležité chápat důležitost **kritického zhodnocení obsahu** internetových stránek. Zřejmé jsou rozdíly mezi stránkami s různým účelem, jako jsou informační stránky, zábavné stránky, blogy, elektronické obchody a jiné. Mezi faktory, podle kterých můžeme posuzovat důvěryhodnost internetových stránek, zejména řadíme: uvedení autora, reference a datum aktualizace obsahu.

Autorské právo a ochrana osobních údajů

Vytvořené dílo je chráněno zákony. **Data i programy** jsou tzv. autorskými díly a jako taková **jsou chráněna autorským zákonem.** Prostřednictvím autorského práva poskytuje stát po jistou omezenou dobu autorům výlučnou možnost rozhodnout o některých aspektech využívání jejich děl. Autorské právo je součástí **duševního vlastnictví** (rozumí se tím výhradní právo k nakládání s díly, vynálezy a jinými nehmotnými výsledky lidské činnosti). Problematiku autorského práva upravuje **zákon č. 121/2000 Sb.,** o právu autorském… (autorský zákon).

Hlavní právní normou, která upravuje ochranu osobních údajů v České republice, je **zákon** č. 101/2000 Sb. **o ochraně osobních údajů.** Podle tohoto zákona si musí každý, kdo shromažďuje osobní údaje a informace za účelem dalšího zpracování, vyžádat k této činnosti souhlas.

Základy on-line komunikace

Internetové komunity

Internetová (virtuální) komunita je tvořena skupinou lidí, ve které její členové navzájem komunikují jinak, než přímým kontaktem. Mezi příklady virtuálních komunit patří např. internetové stránky zájmových skupin, stránky sociálních sítí, internetová fóra, webové konference, chat a komunity hráčů on-line počítačových her. Mezi způsoby, kterými mohou uživatelé zveřejňovat a sdílet informace, patří:

- **blogy (web logy)** – internetový deník,
- **podcasty** – služby pro zveřejňování a automatické stahování zvukových nahrávek a videoklipů z Internetu,
- **internetová alba a archívy** zvukových nahrávek, obrázků a videoklipů.

Důležité je dodržovat **zásady pro zachování osobní bezpečnosti** při práce v internetové komunitě. Každý uživatel by měl:

- vhodně nastavit zabezpečení uživatelského účtu,
- omezit zobrazení osobních údajů,
- preferovat osobní zprávy,
- vypnout informace o vlastní poloze,
- blokovat nebo nahlásit neznámé uživatele.

Komunikační nástroje

Internet nám nabízí různé možnosti komunikace. Komunikace je možná v reálném čase (IM, VoIP, chat), ale nabízí i možnosti, kdy není nutná okamžitá reakce (blog, e-mail, diskusní fóra).

Instant Messaging (IM) – je komunikace v reálném čase. Jedná se o internetovou službu, která umožňuje svým uživatelům sledovat, kteří uživatelé jsou právě připojeni. Podle potřeby jim pak můžeme posílat zprávy, soubory a jinak komunikovat. Nástroje, které umožňují komunikaci v reálném čase: ICQ, Skype, sociální sítě, Windows Live Messenger atd.

Krátkou textovou zprávu (SMS – Short Message Service) lze posílat mezi mobilními telefony, jinými zařízeními, na pevné telefony nebo přes Internet. Technologickým nástupcem SMS jsou zprávy **MMS (Multimedia Message Service),** které umožňují posílat i multimediální obsah.

Voice over Internet Protocol (VoIP) – představuje technologii, která umožňuje přenos digitalizovaného hlasu prostřednictvím internetového protokolu. Využívá se pro telefonování prostřednictvím Internetu, intranetu nebo jakéhokoliv jiného datového spojení. Příklady programů umožňující internetovou telefonii: Skype, Microsoft NetMeeting, atd.

Mezi hlavní návyky pro využívání elektronické komunikace řadíme:

- krátké a stručné vyjadřování,
- používání jednoznačných názvů (předmětů zpráv),
- nezveřejňování osobních informací,
- nerozšiřování nevhodného obsahu,
- kontrolu pravopisu zpráv.

E-mail

Elektronická pošta (e-mail) je způsob odesílání, doručování a přijímání zpráv přes elektronické komunikační systémy. Pomocí elektronické pošty můžeme posílat například dopisy, ale i soubory dat. Velikost přílohy může být omezena. Omezen může být typ odesílaného souboru (spustitelné soubory). Mezi výhody elektronické pošty patří rychlost, cena a ekologičnost.

Při používání e-mailu je třeba dodržovat určitá pravidla etiky, která bývají označována jako **netiketa.** Mezi tato hlavní pravidla řadíme například:

- zprávy posílat vždy **s předmětem mailu**,
- dodržovat pravidla **slušného chování**
- zprávy posílat **bez gramatických chyb**,
- dbát na **přiměřenou velikost příloh** (komprimovat),
- při posílání hromadných e-mailů **dbát na soukromí všech adresátů** (využívat skryté kopie).

Elektronická pošta je zneužívána k posílání **nevyžádaných mailů (spamů)** a různých **podvodných zpráv.** Taková činnost je nelegální, ale velmi těžko postižitelná.

Mezi další rizika používání elektronické pošty patří infekce počítače virem. Uživatel by neměl otvírat nevyžádané maily (zejména přílohy, které většinou při otevření infikují počítač, a to bez vědomí uživatele).

Rozšířenou praktikou je tzv. **phishing.** Jedná se o praktiku, která se snaží od uživatele získat osobní i jiné údaje pod hodnověrnou záminkou.

Každý uživatel elektronické pošty má svou **adresu elektronické pošty.** Taková adresa má povinné části oddělené znakem **@ (zavináč)**.

Při posílání elektronické pošty je zásadní použití různých druhů adresátů:

- **Komu** (To) – standardní pole pro adresu příjemce (můžeme zapsat i více adres, které oddělíme čárkou nebo středníkem),
- **Kopie** (Copy – Cc) – zde můžeme zadat adresy dalších příjemců, každý z nich **bude** po obdržení zprávy **vědět**, kterým dalším osobám byla zpráva poslána v rámci adresátů v polích **Komu** nebo **Kopie**,
- **Skrytá kopie** (Blind Copy – Bcc) – žádný z příjemců, který bude uveden ve skryté kopii, **nebude vědět** o ostatních osobách uvedených v poli **Skrytá kopie** a bude se domnívat, že zpráva byla adresována pouze jemu. Adresát uvedený v poli **Skrytá kopie vidí** ostatní adresáty v polích **Komu** nebo **Kopie**.