



mpc
METODICKO-PEDAGOGICKÉ CENTRUM



Moderné vzdelávanie pre vedomostnú spoločnosť / Projekt je spolufinancovaný zo zdrojov EÚ

RNDr. Monika Molokáčová

Obozretný užívateľ internetových služieb

Osvedčená pedagogická skúsenosť edukačnej praxe

Prešov

2013

Vydavateľ: Metodicko-pedagogické centrum, Ševčenkova 11,
850 01 Bratislava

Autor OPS/OSO: RNDr. Monika Molokáčová

Kontakt na autora: Gymnázium, Poštová 9, Košice, monika.molokacova@gmail.com

Názov OPS/OSO: Obozretný užívateľ internetových služieb

Rok vytvorenia 2013

OPS/OSO:

Odborné stanovisko vypracoval: Mgr. Monika Karol'ová

Za obsah a pôvodnosť rukopisu zodpovedá autor. Text neprešiel jazykovou úpravou.

Táto osvedčená pedagogická skúsenosť edukačnej praxe/osvedčená skúsenosť odbornej praxe bola vytvorená z prostriedkov národného projektu Profesionálny a kariérový rast pedagogických zamestnancov. Projekt je financovaný zo zdrojov Európskej únie.

Kľúčové slová

internet, komunikácia, internetové služby, bezpečnosť, riziká, informačná spoločnosť

Anotácia

Osvedčená pedagogická skúsenosť edukačnej praxe predstavuje metodiku vyučovania internetových služieb založenú na konštruktivistických princípoch vyučovania. Využíva najmä aktivizujúce metódy, skombinované do netradičnej formy „moderovanej debaty“, v ktorej stoja proti sebe dvaja žiaci – „zástanca“ a „odporca“ nastolenej tézy z oblasti bezpečnosti internetových služieb. Moderátorom je učiteľ, v role porotcov sú práve nedebatujúci spolužiaci. Metodika bola overená vo vyučovaní informatiky na gymnáziu, súčasťou práce je tiež súhrn postrehov, ktoré vyplynuli z vyučovania podľa nej.

OBSAH

ÚVOD	4
1 OPIS OSVEDČENEJ PEDAGOGICKEJ SKÚSENOSTI	5
2 PLÁNOVANIE VYUČOVANIA	7
2.1 Konštruktivistické prístupy k vyučovaniu	8
2.2 Aktivizujúce metódy	8
2.2 Didaktická analýza návrhu metodiky	9
3 SLUŽBY INTERNETU – NÁVRH METODIKY	11
3.1 Fáza prípravy	11
3.2 Techniky sociálneho inžinierstva	15
3.3 Fáza realizácie	20
4 VÝSLEDKY MODEROVANEJ DEBATY	23
4.1 Publikovanie a vyhľadávanie informácií na webe	23
4.2 Ukladanie, prenos a zdieľanie údajov	25
4.3 Elektronické kancelárie, pobočky, obchody	27
4.4 Komunikačné služby	29
4.5 Sociálna sieť	32
ZÁVER	36
Zoznam bibliografických zdrojov	37

ÚVOD

Akčný plán stratégie informatizácie spoločnosti v podmienkach Slovenskej republiky v časti Vzdelávanie a zamestnanosť, okrem iného uvádza: „Úlohou moderného vzdelávacieho procesu je zabezpečiť, aby prakticky každý občan bol informačne gramotný, mal prístup k internetu a pociťoval výhody informačnej spoločnosti“. Považujeme však za rovnako dôležité formovať u žiakov obozretnosť a opatrnosť na základe znalosti rizika súvisiaceho s užívaním výhod informačnej spoločnosti. Každý žiak by mal vnímať sociálne a technologické riziká používania informačných technológií a vedieť sa brániť sociálnym, aj technologickým hrozbám v súvislosti s používaním služieb internetu.

V bežnom živote ľudia často využívajú služby internetu bez zváženia hrozieb, ktoré sú s ich užívaním spojené. V navrhnutej metodike chceme poukázať na možnosť zaradiť situácie z praktického života do vyučovania informatiky, vyťažiť z týchto situácií v záujme premeny tradičného, inštruktívneho vyučovania informatiky smerom k aktívnemu konštruovaniu žiackych spôsobilostí. Uplatnenie vytvoreného systému úloh podľa navrhnutej metodiky má za cieľ motivovať žiakov, podporiť ich tvorivosť, chuť skúmať a experimentovať, kriticky zhodnotiť postoje iných žiakov.

Metodika je pre vyučovanie informatiky prínosom najmä v podobe zatraktívnenia učiva, rozvoja kritického myslenia a hodnotiaceho posúdenia žiakov podnecovaním k skúmaniu a formulácii vlastných záverov, podnecovania žiakov k efektívnemu a obozretnému využívaniu moderných technológií, zlepšenia sociálnych, komunikačných a interpersonálnych zručností žiakov, demokratizácie vzťahu „učiteľ – žiak“ a tým aj celkovej klímy výchovno-vzdelávacieho procesu.

Jadro práce je rozdelené do štyroch kapitol. Obsahom prvej kapitoly je stručná charakteristika osvedčenej pedagogickej skúsenosti, v druhej kapitole sú zosumarizované teoretické východiská návrhu metodiky, ktoré predstavujú súhrn aktuálnych poznatkov k danej téme, získaných štúdiom dostupných literárnych zdrojov. V rámci kapitoly vymedzujeme základné pojmy týkajúce sa problematiky metód vyučovacieho procesu, charakterizujeme aktivizujúce metódy. Zaoberáme sa výhodami aj nevýhodami ich uplatnenia vo výučbe, porovnaním pohľadov z rôznych zdrojov sa snažíme o zachovanie objektivity.

Rozsiahlejšia tretia a štvrtá kapitola podrobne opisuje navrhnutú metodiku vyučovania, opisuje činnosť žiakov, učiteľa, predpoklady aj výsledky spojené s realizáciou moderovanej debaty vo vyučovaní informatiky. Obsahuje tiež súhrn našich postrehov, ktoré vyplynuli z vyučovania podľa metodiky.

1 OPIS OSVEDČENEJ PEDAGOGICKEJ SKÚSENOSTI

Kontext a rámec

Metodika predstavená v jadre tejto práce bola opakovane overená v rámci vyučovania povinného predmetu informatika na gymnáziu, v triedach prvého a druhého ročníka so všeobecným zameraním. V súlade so štátnym vzdelávacím programom (ďalej ŠVP) a školským vzdelávacím programom (ďalej ŠkVP) sa v týchto triedach týždenne vyučujú dve hodiny informatiky.

Škola disponuje tromi multimediami počítačovými učebňami, ktoré sú ťažiskovo využívané na vyučovanie informatiky. Vo všetkých učebniach školy je možné využiť datavideoprojekciu. Učitelia majú v každej predmetovej komisii k dispozícii aspoň jeden prenosný počítač.

Špecifikácia cieľovej skupiny

- kategória, resp. podkategória pedagogických a odborných zamestnancov podľa zákona č. 317/2009. Z. z.: učiteľ pre nižšie stredné odborné vzdelávanie, stredné odborné vzdelávanie, úplné stredné všeobecné vzdelávanie, úplné stredné odborné vzdelávanie a učiteľ pre vyššie odborné vzdelávanie (učiteľ strednej školy)
- vzdelávacia oblasť: *matematika a práca s informáciami*
- škola, ročník: *gymnázium, 1. – 2. ročník*
- vyučovací predmet: *informatika*
- tematický okruh: *obsah zasahuje do dvoch navzájom súvisiacich okruhov ŠVP: Komunikácia prostredníctvom IKT a Informačná spoločnosť*
- tematický celok, učivo: *Služby internetu. Neinteraktívna komunikácia – e-pošta, diskusné fórum, blog. Interaktívna komunikácia. Web – prehliadače, webová stránka, vyhľadávanie informácií. Netiketa. Bezpečnosť na internete. Sociálne siete. Web2.0. Riziká informačných technológií – malvér (pojmy, detekovanie, prevencia); kriminalita. Etika a právo – autorské práva na softvér, licencia (freeware, shareware, demoverzia, multilicencia, open source.).*

Cieľ práce

Metodicky opísať vyučovanie s uplatnením aktivizujúcich metód a netradičných foriem vo vyučovaní tematických okruhov Komunikácia prostredníctvom IKT a Informačná spoločnosť, v témach „Služby internetu“, „Bezpečnosť a riziká informačných technológií“, s dôrazom na aktívne včlenenie žiaka do procesu vzdelávania.

Vymedzenie kompetencií

Prostredníctvom netradičnej formy práce, moderovanej debaty, ktorá od účastníkov: žiaci debatéri - zástanca a odporca, nedebatujúci žiaci porotcovia, vyžaduje zdatnosť v diskutovanej problematike, zdatnosť v argumentácii, prezentačné zručnosti, kritické

myslenie a schopnosť hodnotiť a posudzovať, formulovať závery. Prostredníctvom zvolených káuz a téz z reálneho sveta nenútené budujeme medzipredmetové vzťahy, formujeme postojovú orientáciu žiakov a posilňujeme kompetencie uplatňovať kritické myslenie, kompetencie v oblasti riešenia problémov, argumentácie, komunikácie, posudzovania, hodnotenia, sebahodnotenia, učebné, pracovné, v oblasti IKT.

2 PLÁNOVANIE VYUČOVANIA

Učivo tematického celku „Služby internetu“ patrí k základnej informačnej gramotnosti človeka, ktorú „možno zjednodušene charakterizovať ako schopnosť jednotlivca identifikovať, vyhľadať, hodnotiť a používať informácie. Je jedným zo základných aspektov civilizačnej gramotnosti súčasného človeka a súvisí s požiadavkami súčasnej modernej spoločnosti, ktorá je vyšpecifikovaná ako informačná spoločnosť.“ [1] Vo väčšine školských vzdelávacích programov je jeho obsah v učebných osnovách rozvrhnutý na prvé dva ročníky gymnaziálneho štúdia.

Učivo tematického celku „Bezpečnosť a riziká informačných technológií“ úzko súvisí s učivom okruhu „Komunikácia prostredníctvom IKT“, nadväzuje však aj na ostatné tematické okruhy gymnaziálnej informatiky. Zaoberá sa etickými, morálnymi a spoločenskými aspektmi informatiky. Oboznamuje s možnými rizikami a metódami na riešenie týchto rizík. Žiaci by sa mali oboznámiť s využitím IKT v najrôznejších oblastiach vedomostnej spoločnosti, pochopiť, že používanie IKT si vyžaduje kritický a zvažujúci postoj k dostupným informáciám. Vo väčšine školských vzdelávacích programov je jeho obsah v učebných osnovách zaradený až do tretieho, či dokonca štvrtého ročníka gymnaziálneho štúdia.

Máme za to, že formovanie informačne obozretného žiaka, ktorý

- vie efektívne selektovať dostupné nástroje internetu,
- vie vyhýbať sa a odolať nástrahám internetových služieb,
- vie posúdiť dôveryhodnosť a relevantnosť internetových informačných zdrojov,

by nemalo byť odsunuté na záver gymnaziálneho štúdia, ale malo by byť nenásilne implementované do vyučovania všetkých tematických okruhov informatiky, už od prvého ročníka.

Podporou tohto zámeru sú alarmujúce výsledky niekoľkých testovaní v oblasti informačnej gramotnosti mladých ľudí. Bezpečnostná firma ESET v spolupráci so svojou divíziou ESET Services vytvorila pre účely „IT fitness testu národa 2012“ vedomostno-behaviorálny dotazník. Časť dotazníka sa týkala konkrétneho správania testovaných, teda ich vedomostí v oblasti počítačovej bezpečnosti, druhá časť analyzovala dôsledky správania sa testovaných. Z výsledkov vyplynulo, že napriek tomu, že takmer všetci účastníci testu vedeli, čo je nevyžiadaná pošta, v praktickom teste už svoje teoretické vedomosti nezúročili. Ukázalo sa, že:

- len 7 percent opýtaných mladých ľudí, pre ktorých bol test primárne určený, správne vyhodnotilo mail, ktorého obsahom bol phishing,
- priemerný mladý Slováč je náchylný k tomu, aby nesprávne vyhodnotil e-mail, ktorý od neho žiada citlivé údaje,
- každý piaty mladý Slováč sa na internete stretol so zneužitím svojich údajov,
- 65 percent opýtaných má skúsenosť s napadnutím svojho počítača, ktoré mohlo byť spôsobené nezodpovednou prácou v režime administrátora,
- 15 percent opýtaných potvrdilo, že ich počítač je napadnutý niekoľkokrát do roka. [3]

Kritickým a tradičným problémom slovenského školstva doloženým už z osemdesiatych rokov je nedostatočná spôsobilosť študentov aplikovať vedomosti nadobúdané v škole

pri riešení konkrétnych problémov. Podľa Výskumného programu OECD na medzinárodné hodnotenie študentov PISA [8] (Programme for International Student Assessment) boli výsledky slovenských študentov v skupine „Riešenie problémov“ pod priemerom OECD. [1]

Tieto zistenia jednoznačne poukazujú na potrebu inovácie vyučovacích stratégií smerom k podpore aktivity a angažovanosti žiakov v procese vzdelávania, v záujme zvyšovania vyššie definovanej informačnej gramotnosti žiakov. To je plne v súlade s požiadavkou ŠVP: „Pri voľbe metód vyberáme moderné vyučovacie metódy, ktoré podnecujú žiakov k aktívnejšiemu prístupu.“

Konstruktivistické prístupy k vyučovaniu

Tendencia objavovať alternatívne vyučovacie metódy s cieľom prekonať neaktuálne postupy a zvyšovať efektivitu učenia sa, je odnepamäti súčasťou procesu výchovy a vzdelávania, a prirodzene pretrváva aj v súčasnosti. Zároveň si však uvedomujeme, že určité druhy metód sú rovnako odnepamäti vlastné vyučovaciemu procesu. Maňák [9] ich označuje prívlastkom „tradičné“ a nechápe ich ako „metódy vývojovo prekonané, už zastarané alebo v krátkom čase odsúdené k zániku“, ale skôr tak, že „tieto metódy sú ustálené, overené praxou“. Tieto tiež prechádzajú procesom modernizácie a spolu s novými metódami sú nenahraditeľným nástrojom učiteľov.

Aktivizujúce metódy

Všetky moderné koncepcie vyučovacieho procesu sa zhodujú v tom, že žiak musí byť vo vyučovacom procese motivovaný a aktívny, že je nevyhnutné odstrániť pasivitu študentov, typickú pre tradičné vyučovanie. Protikladom tradičnej školy je koncepcia konstruktivismu, kde nachádzajú uplatnenie aktivizujúce a komplexné vyučovacie metódy z vyššie uvedenej klasifikácie. Charakteristické pre túto koncepciu je, že žiak sám zvažuje nové informácie, porovnáva ich s predchádzajúcimi skúsenosťami, prispôsobuje a pretvára tieto nové informácie tak, aby mu dávali zmysel z hľadiska toho, čo už vie, čím aktívne konštruuje svoje poznanie. Aj od učiteľa sa vyžaduje aktívny prístup a tvorivosť, učiteľ sa stáva partnerom žiaka. To má za následok priaznivý vplyv na klímu triedy, v komplexnom ponímaní aj klímu školy. Svojím charakterom sú aktivizujúce metódy nezastupiteľné pri rozvoji funkčnej gramotnosti a hodnotového systému žiakov vďaka tomu, že ich uplatnenie v procese vzdelávania prirodzene vedie žiakov:

- k cielenému hľadaniu nových poznatkov,
- k spochybňovaniu a nedôvere voči informačným zdrojom bez porozumenia,
- k potrebe argumentácie a zdôvodňovania,
- k objavovaniu vzájomných súvislostí medzi poznatkami bez ohľadu na učebný predmet,
- k dôvere vo vlastné schopnosti,
- k uplatňovaniu vlastného myslenia a nových nápadov,
- k overovaniu netradičných myšlienok, aj tých, ktoré sú v rozpore s uznávanými pravdami,
- k vytvoreniu a vyjadreniu vlastného pohľadu na svet,
- k spolupráci v skupine,
- k formovaniu interpersonálnych vzťahov na rôznych úrovniach.

Výučba so zaradením aktivizujúcich metód kladie vysoké nároky na učiteľa aj na žiakov. Je potrebné ju starostlivo pripraviť a k jej úspešnej realizácii je nutná spolupráca všetkých žiakov a učiteľa. Ako sme uviedli v prvej kapitole, voľba metódy vyučovacieho procesu je dynamicky viazaná na ostatné kategórie vyučovacieho procesu. „Výber metódy musí byť podriadený učivu, žiakom, učiteľovi (jeho skúsenostiam), v neposlednom rade aj pomôckam a didaktickej technike, ktorú má učiteľ k dispozícii, organizačnej forme vyučovania“... [11].

2.3 Didaktická analýza návrhu metodiky

Obsahový plán opísaného vyučovania vychádza z obsahového a výkonového štandardu prílohy ISCED 3A štátneho vzdelávacieho programu predmetu informatika. V ňom uvedené univerzálne aj špecifické požiadavky sa premietli do samotného výchovno-vzdelávacieho procesu vymedzením didaktických charakteristík uvedených v tabuľke 1.

Tabuľka 1 Základné charakteristiky návrhu metodiky

<i>Téma</i>	<i>Ročník</i>
Služby internetu Bezpečnosť a riziká informačných technológií	Prvý, druhý SŠ
<i>Ciele</i>	<i>Vstup</i>
<ul style="list-style-type: none"> • poznať služby internetu • mať užívateľské zručnosti v užívaní služieb internetu • vnímať sociálne riziká používania informačných technológií • brániť sa sociálnym hrozbám v súvislosti s používaním služieb internetu • vnímať technologické riziká používania informačných technológií • brániť sa technologickým hrozbám v súvislosti s používaním služieb internetu • rešpektovať intelektuálne vlastníctvo a autorstvo informatických produktov, systémov a aplikácií • poznať druhy softvérového pirátstva • poznať sociálne, etické a právne dôsledky neakceptovania autorských práv • poznať a dodržiavať pravidlá netikety • podieľať sa na práci v skupine • akceptovať názory iných členov skupiny • prezentovať a obhájiť výsledky samostatnej práce • zhodnotiť prezentované riešenia spolužiakov 	<ul style="list-style-type: none"> • chápať význam pojmov informácia, údaj, počítač, sieť, internet, komunikácia, bezpečnosť, riziko, škodlivý softvér • mať zručnosti vo vyhľadávaní informácií • mať prezentačné zručnosti

<i>Kompetencie</i>	<i>Didaktický problém</i>
<ul style="list-style-type: none"> • špecifikovať problém, selektovať relevantné údaje • využiť vhodný IKT nástroj na reprezentáciu a skúmanie údajov • interpretovať objavené vzťahy • argumentovať a zdôvodňovať • kriticky posúdiť • hodnotiť • komunikovať 	<ul style="list-style-type: none"> • Kritickým problémom slovenského školstva je nedostatočná spôsobilosť žiakov aplikovať vedomosti nadobúdané v škole pri riešení konkrétnych problémov. Výskumy potvrdili, že sa to týka aj oblasti bezpečného správania sa žiakov pri využívaní internetových služieb. Ponúkané riešenie má za cieľ aktivizovať žiakov pri osvojovaní vedomostí, formovať ich návyky a postoje v danej oblasti.
<i>Prostriedky</i>	<i>Metódy a formy</i>
<ul style="list-style-type: none"> • počítač • prezentačná technika 	<ul style="list-style-type: none"> • konštruktivistické prístupy k učeniu • aktivizujúce metódy

Prameň: vlastný návrh

3 SLUŽBY INTERNETU – NÁVRH METODIKY

V návrhu metodiky sú kombinované viaceré konštruktivistické metódy a formy práce, najmä inscenačné, situačné, diskusné metódy, a tiež problémové vyučovanie. Súhrnne sme pre použité metódy a formu zaviedli označenie moderovaná debata. Činnosť učiteľa a žiakov je rozdelená do dvoch fáz debaty, fázy prípravy a fázy realizácie.

3.1 Fáza prípravy

Úlohou učiteľa v prípravnej fáze je podľa počtu žiakov v skupine pripraviť témy a k nim východiskové kauzy. Kauzy nevyčerpávajú tému, ich cieľom je navodiť situáciu pre diskusiu, debatu, prípadne polemiku. Kauzy by preto mali byť verejnosti dostatočne známe, medializované, pre potrebu opisovanej formy vyučovania boli volené účelne a prvoplánovo. V našej skupine bolo desať žiakov, preto sme problematiku internetových služieb rozdelili do piatich oblastí - tém:

1. publikovanie a vyhľadávanie informácií na webe,
2. ukladanie, prenos a zdieľanie údajov,
3. elektronické kancelárie, pobočky, obchody,
4. komunikačné služby,
5. sociálna sieť.

Ku každej téme sme vyhľadali aktuálnu kauzu, ktorá bola podnetom pre formuláciu kontroverzného tvrdenia, tzv. debatnej tézy.

1. Publikovanie a vyhľadávanie informácií na webe

Téza: „Sledovanie užívateľskej činnosti na webe by malo byť zakázané.“

Google o vás vie viac

„Štvrtok 1. marca 2012 zůstane provždy dnem, kdy se internet pro miliony uživatelů nenápadně, ale podstatně změnil. Počínaje tímto dnem Google upravil svá Pravidla na ochranu soukromí.

Google je ode dneška legálně schopen - pokud se přihlásíte na jakoukoli jeho službu - zkombinovat informace ve váš velmi podrobný osobnostní profil. Může být složený z informací o místě, kde se nacházíte, z vašich zájmů a oblíbených témat, informací o vaší současné práci i celé kariéře, přátelích, online návycích i třeba společenských kruzích, ve kterých se pohybujete.

Díky tomu vám bude YouTube doporučovat videa pozoruhodně se trefující do vašeho vkusu a stejně to bude i s reklamami. To, co nakoupí vaši přátelé ze sociální sítě Google Plus zase bude mít vliv na reklamy, které se vám objevují při vyhledávání.“

<http://datarama.aktualne.centrum.cz/clanek.phtml?id=735386>

2. Ukladanie, prenos a zdieľanie údajov

Téza: „Cloudové úložiská sú centrá počítačového pirátstva a napomáhajú plagiátorstvu.“

Cloudové úložisko Mega

„Presne po roku od vypnutia obľúbenej a populárnej služby na zdieľanie dát Megaupload.com dnes Kim Dotcom a jeho tím oficiálne spustil kompletne prepracovanú cloudovú službu s názvom Mega.

Ako sme informovali už v starších článkoch, na rozdiel od pôvodného Megauploadu budú súbory nahrané do Mega šifrované pomocou algoritmu Advanced Encryption Standard (AES). Používateľ, ktorý daný súbor do služby nahrá, získa unikátny kľúč pre jeho dešifrovanie. Kľúč môže následne poslať tomu, kto si ho bude chcieť stiahnuť.

Dešifrovací kľúč ale nebude uložený v samotnej službe a jej prevádzkovatelia tak nebudú mať možnosť vidieť akýkoľvek súbor nahraný na serveroch. Týmto krokom sa chce Mega zbaviť zodpovednosti za nahrané súbory a presunúť ju na používateľov. „Ak niekto servery ukradne alebo hackne, neposkytnú mu žiadne informácie,“ uviedol Dotcom.

Mega bude dohliadať aj na porušovanie autorských práv. „Ak držiteľ práv nájde na internete odkazy na súbory aj s ich dešifrovacími kľúčmi a overí, že súbor skutočne porušuje ich práva, môže nám poslať žiadosť na jeho odstránenie,“ uviedol Mathias Ortmann, zamestnanec Megauploadu a Dotcomov partner v službe Mega.“

<http://www.zive.sk/odstartovalo-mega-ulozisko-dotcoma-ponuka-4-terabajty/sc-3-a-306463/default.aspx?showforum=1>

3. Elektronické kancelárie, pobočky, obchody

Téza: „Nákupom v internetovom obchode vedome podstupujeme riziko podvodu.“

Škoda za desiatky tisíc

„Desiatky ľudí sa dali pred Vianocami zlákať na podozrivo nízke ceny, ktoré ponúkal internetový obchod Lacnokup.eu a sesterský zľavový portál TopSales.sk. Trenčianskej firme Kronix, ktorá ich prevádzkuje, zaplatili, no tovaru sa nedočkali.

Tablet Samsung Galaxy Tab 10.1 ponúkal tento eshop v akcii za 299 eur. Jeho bežná cena pritom býva vyššia ako 400 eur. Za takmer polovičné ceny predával spotrebiče, fotoaparáty aj parfumy.

Spotrebiteľské centrum eviduje 90 ľudí, ktorých e-shop poškodil. Mohol zhltnúť desaťtisíce eur.“

<http://ekonomika.sme.sk/c/6196234/lacny-tovar-mohol-byt-podvod.html>

4. Komunikačné služby

Téza: „Diagnóza závislosti od internetu nie je odborné uznaná, problém je zveličený, psychicky zdravých ľudí neohrozuje.“

Odobranie detí

„Triaťricetiletá Polka byla soudem odsouzena k psychiatrické léčbě a odebrání dětí, jelikož mimo internetového připojení neplatila žádné účty a její jedinou činností bylo surfování po diskusních serverech.

Na svou obhajobu uvedla, že se dostala po rozvodu do deprese, jíž se zbavovala právě díky chatování s internetovými přáteli.“

<http://www.nebudobet.cz/?page=netholismus>

5. Sociálna sieť

Téza: „Rozmach sociálnych sietí podporuje rozmach sociálnych deviácií a kyberkriminality.“

Sociálne siete sú najrizikovejšie miesto na internete

„Nedávna správa bezpečnostnej firmy Sophos hodnotiaca rok 2010 odhalila, že najväčšie bezpečnostné riziko na internete v súčasnosti prichádza zo stránok sociálnych sietí ako sú Facebook, Twitter, LinkedIn, či MySpace.

Najväčšia sociálna sieť na internete, Facebook, má v súčasnosti viac ako 800 miliónov aktívnych užívateľov. Viac ako 50 percent z nich sa na svoje konto prihlasuje každý deň. Ľudia denne okomentujú alebo označia, že sa im páčia, viac ako dve miliardy postov - to predstavuje lukratívny potenciálny trh nielen pre spoločnosti, ale v čoraz vyššej miere aj pre podvodníkov. Používatelia sú tak dnes často vystavení bezpečnostnému riziku - najmä vplyvom skutočnosti, že ich profil na sociálnych sieťach často obsahuje citlivé osobné údaje.

V poslednom čase sa tak na internete objavuje čoraz viac prípadov kyberkriminality. Jedným z nástrojov je ClickJacking. Ako uvádza blog Synopsi, ide o formu útoku, pri ktorej útočník prekryje jednu web stránku druhou. Používateľ a potom naláka, aby klikol na tlačítko „Páči sa mi“ alebo v prípade videa na jeho prehratie. Ak tak ale spraví, neotvorí sa im žiadaná stránka, no na ich profil sa pridá útočníkom vopred vybraná stránka a je tak prístupná a odporúčaná jeho priateľom.

Ak už útočník nazbiera dostatočný počet takýchto užívateľov, môže na pôvodný link pridať malware a tým sa dostať do počítača obetí. Príkladmi ClickJackingu sú stránky, ktoré lákajú už svojim názvom, ako napríklad: „Pozrite si najsmiešnejšie video na svete“, či „Po tomto videu už nikdy nebudete chcieť piť Coca Colu“, pričom po kliknutí naň si od užívateľa vypýtajú súhlas k prístupu k jeho verejným informáciám a k zverejneniu na jeho stránke.

<http://www.euractiv.sk/bezpecny-internet/clanok/socialne-siete-su-najrizikovejsie-miesto-na-internete-017939>

Ku každej takto zostavenej téze sme priradili dvoch žiakov, účastníkov moderovanej debaty. Jedného „zástancu“ (na strane „ZA“ tézu), ktorého úlohou bolo vyhľadať a predstaviť súhlasné argumenty podporujúce tvrdenie tézy. Jedného „odporcu“ (na

strane „PROTI“ téze), ktorého úlohou bolo vyhľadať a predstaviť nesúhlasné argumenty odporujúce tvrdeniu tézy. Toto pridelenie žiakov nebolo verejné, úlohou žiakov bolo držať svoju rolu v tajnosti a postarať sa o zabezpečenie všetkých dát a materiálov pripravených na fázu realizácie.

Je dôležité uvedomiť si, že žiaci si problematiku ani postoj nevyberajú podľa svojho presvedčenia, v moderovanej debata potom musia zastávať pozíciu, ktorá im je vopred určená. Sú tak postavení do pozície, kedy musia argumentovať v prospech istého postoja a vymyslieť najlepší spôsob, ako takýto postoj obhájiť. Vďaka tomu sú nútení premýšľať o pridelenej problematike z viacerých strán, predvídať opačné názory a argumenty, vypočítať ich a byť pripravený kultivovane na nich reagovať.

Motiváciou pre výkony žiakov je súťaživý charakter moderovanej debaty, kde jedna strana vyhrá, druhá teda nutne musí prehrať, pričom porotcami sú všetci nedebatujúci prítomní spolužiaci. Regulárnosti hlasovania poroty napomáha utajenie pripravených materiálov, utajenie zastávaného postoja, ktorého cieľom je okrem iného zabrániť ovplyvňovaniu „poroty“ pred samotnou realizáciou debaty. Konečný výsledok debaty, výhra/prehra odporcu/zástancu, samozrejme nemá vplyv na hodnotenie výkonu žiakov učiteľom.

Vzhľadom k tomu, že cieľom debaty nie je iba diskusia o téze, inšpirovaná predloženou kauzou, ale tiež rozšírenie pohľadu na celú problematiku, predstavenie internetových služieb spolužiakom, vrátane možných rizík spojených s ich používaním, podmienkou vystúpenia žiakov bola pripravená počítačová prezentácia, resp. samostatné digitálne materiály. Na rozdiel od akademickej debaty pomocou nich prostredníctvom projekcie demonštrovali a podporovali predkladané argumenty. Preto v prípravnej fáze učiteľ okrem tézy a kauzy žiakom odovzdal aj osnovu, v ktorej zosumarizoval hlavné internetové služby zaradené do okruhu k príslušnej téze. Následne, v stanovenom čase pred fázou realizácie, žiaci odovzdali všetky pripravené materiály učiteľovi na konzultáciu, ktorý v záujme obsahového vyčerpania témy, či vyrovnania veľkých rozdielov medzi „zástancom“ a „odporcom“, nasmeroval žiakov k doplneniu, resp. vhodnej forme prípravy.

Osnovy k témam, ktoré učiteľ poskytne obom debatérom („zástancovi“ aj „odporcovi“) spolu s kauzou a tézou:

1. Publikovanie a vyhľadávanie informácií na webe:
 - a. webový prehliadač,
 - b. vyhľadávacie nástroje na internete: katalógy, vyhľadávacie roboty, metavyhľadávače,
 - c. spôsoby zadávania vyhľadávacích dopytov,
 - d. špecializované vyhľadávanie,
 - e. publikovanie prostredníctvom vlastného webu,
 - f. publikovanie prostredníctvom blogu,
 - g. publikovanie vo wiki – systéme.

2. Ukladanie, prenos a zdieľanie údajov:
 - a. FTP,
 - b. dátová úschovňa,

- c. cloudové úložisko,
 - d. cloud computing,
 - e. streaming,
 - f. podcast.
3. Elektronické kancelárie, pobočky, obchody:
- a. elektronická verejná správa (eGovernment),
 - b. portály verejných inštitúcií,
 - c. elektronické bankovníctvo,
 - d. elektronický obchod.
4. Komunikačné služby:
- a. zasielanie okamžitých správ (instant messaging),
 - b. chat,
 - c. hlasový chat (voice chat),
 - d. videokonferencia,
 - e. IP telefonovanie,
 - f. e-mail,
 - g. elektronický distribučný zoznam (electronic mailing list),
 - h. internetové fórum.
5. Sociálna sieť:
- a. kontakty,
 - b. politika ochrany súkromia,
 - c. publikovanie v sociálnej sieti,
 - d. komunikačné nástroje sociálnej siete.

Posledným krokom, ktorý sme vo fáze prípravy zabezpečili, bola dohoda so žiakom tej istej triedy, avšak inej skupiny v rámci rozdelenia na vyučovaní informatiky, ktorý zohrával prísne utajenú rolu „agenta“. Jeho úloha spočívala vo všemožnej snahe nepozorovane sa dostať k informáciám od pripravujúcich sa žiakov, ktorí ich mali udržať v tajnosti. Pri výbere žiaka je treba zohľadniť jeho postavenie v triede, je dôležité aby disponoval sociálnymi kompetenciami, bol komunikatívny, diplomatický, rozhodný, v plnení tejto funkcie voči učiteľovi lojálny (a nelojálny k spolužiakom), vnímavý. Ak sa „agentovi“ podarí získať údaje napriek utajeniu, ide o praktickú ukážku „sociálneho inžinierstva“ v prostredí triedy. Zvoleného „agenta“ sme oboznámili s praktikami sociálneho inžinierstva, ktoré sme neskôr predstavili celej skupine žiakov.

„Virtuálnym agentom“ môže byť aj učiteľ, ktorý sa prostredníctvom phishingu pokúsi získať údaje od žiakov. V našom prípade sme použili phishing prostredníctvom elektronickej komunikácie. Z novovytvoreného e-mailového účtu, ktorého adresa bola odvodená od mena učiteľa, v záujme dôveryhodnosti bola informácia o odosielateľovi nastavená ako meno učiteľa, sme v termíne tesne pred fázou realizácie, kedy sme predpokladali, že žiaci už majú materiál pripravený, požiadali o jeho zaslanie na „finálnu kontrolu spojenú s hodnotením“.

3.2 Techniky sociálneho inžinierstva

Sociálne inžinierstvo (sociotechnika) je postup, akým útočník, v ktorého úlohe môže byť v podstate ktokoľvek a v akejkolvek situácii, využije manipuláciu človeka za účelom

získania istých pre neho prospešných informácií dôverného charakteru alebo za účelom prinútenia človeka k vykonaniu požadovanej akcie (činnosti). Techniky sociálneho inžinierstva možno aplikovať v akejkol'vek oblasti života, v súčasnosti zaznamenávajú rozmach informácie, ktoré majú spojitosť s oblasťou informačných technológií.

Tento spôsob útokov na organizácie, či jednotlivcov, a získavania informácií býva veľmi úspešný. Aj napriek tomu, že si nevyžaduje takmer žiadne špeciálne technické znalosti a technologické prostriedky. Sociálne inžinierstvo sa svojimi metódami a praktikami snaží využiť hlavne faktory, ktoré ovplyvňujú ľudské správanie a rozhodovanie. Faktory, ktorými môže byť človek ovplyvňovaný, sú: dôvera, rešpektovanie autorít, súcit, potreba vyhnutia sa konfliktu, potreba „mať pokoj“, sympatie, stres a ďalšie. V našom prípade sme útok postavili na prvých dvoch faktoroch: dôvera k spolužiakovi a rešpektovanie autority učiteľa.

Sociálne inžinierstvo je skutočne len o ľuďoch, o miere ich dôverčivosti, inteligentnosti, či dedukcii. Úlohou útočníka je využiť všetky prostriedky na to, aby sa dostal k požadovaným údajom. Na to musí byť samozrejme tiež dostatočne inteligentný, presvedčivý a v neposlednom rade aj trpezlivý.

Je všeobecne známe, že bezpečnosť akéhokolvek, teda aj počítačového systému, je určená bezpečnosťou jeho najslabšieho článku. Sociálne inžinierstvo stavia svoj útok na tom, že najslabším článkom systému je spravidla človek. Vo firemnom prostredí môžeme za najslabší článok konkrétne označiť zamestnancov. Istí zamestnanci vždy pracujú so zaujímavými dátami a samozrejme mnohokrát sa stane, že nedodržia bezpečnostnú politiku resp. nedajú na pravidlá, ktoré im nariadil administrátor. I keď sa v určitých organizáciách žiaľ objavujú aj prípady, kde sociálne inžinierstvo mnoho administrátorovi nehovorí, alebo čo je ešte horšie, nehovorí mu nič ani pojem bezpečnostnej politiky. Vďaka osvete a vzdelávaniu v tejto oblasti si však riziká plynúce z kybernetických hrozieb uvedomuje stále viac ľudí.

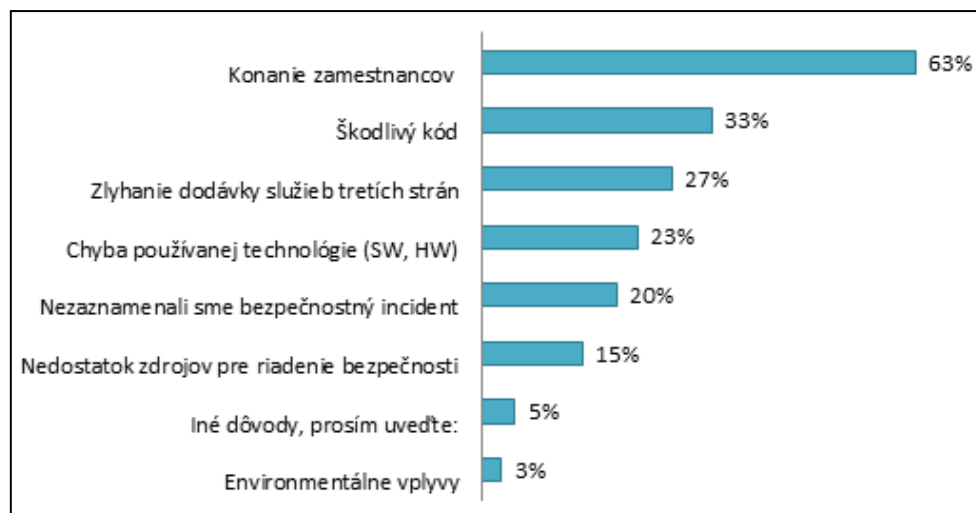
Známe prípady útokov sociálneho inžinierstva:

- Prienik do siete Medzinárodného menového fondu (MMF).
- Únik (v tom čase) nového dielu Harryho Pottera.
- Únik úloh maturitných testov.
- Falošný telefonát dvoch moderátorov, ktorí sa vydávali za britskú kráľovnú Alžbetu II. a princa Charlesa, boli prepojení do nemocničnej izby vojvodkyne z Cambridgeu, Kate.
- Účtovníčka nemenovanej stavebnej firmy z Nových Zámkov dostala od údajného šéfa spoločnosti SMS, aby okamžite uhradila vysokú faktúru a súčasne jej prišiel e-mail s faktúrou, ktorá bola v SMS spomenutá, firma úhradou prišla o 50 000 eur.
- Spoločnosť F-Secure odhalila e-mail, ktorým prenikli útočníci do siete spoločnosti RSA. Táto kauza bola patrične vážna. Hackeri použili phishingový e-mail, ktorý zaslali zamestnancom, jeho predmet niesol názov "2011 Recruitment Plan," v prílohe obsahoval súbor "2011 Recruitment plan.xls." (V preklade: Náborový plán 2011.) Telo e-mailu obsahovalo jednoduchý text: "I forward this file to you for review. Please open and view it." (V preklade: Posielam tento súbor na

preverenie, prosím otvorte ho a pozrite sa naň.) Odosielateľom bola e-mailová adresa webmaster@beyond.com, služba Beyond sa zaoberá hľadaním zamestnancov. Samotný .xls súbor obsahoval Flash objekt zneužívajúci toho času ešte neznámu bezpečnostnú zraniteľnosť CVE-2011-0609, ktorá sa týkala Adobe Flash Playera. Hackerom tak umožnila integráciu backdoora do systémov obetí. Podvodný e-mail mal byť odoslaný minimálne štyrom zamestnancom spoločnosti. Útočník si veľa námahy s prácou na podvode nedal, no i tak boli následky obrovské. Zamestnanci totiž daný súbor otvorili a tým umožnili odcudzenie údajov ohľadne autentizačného nástroja SecurID, ktoré neskôr viedlo k útokom na rôzne významné spoločnosti, ako Lockheed Martin. [7]

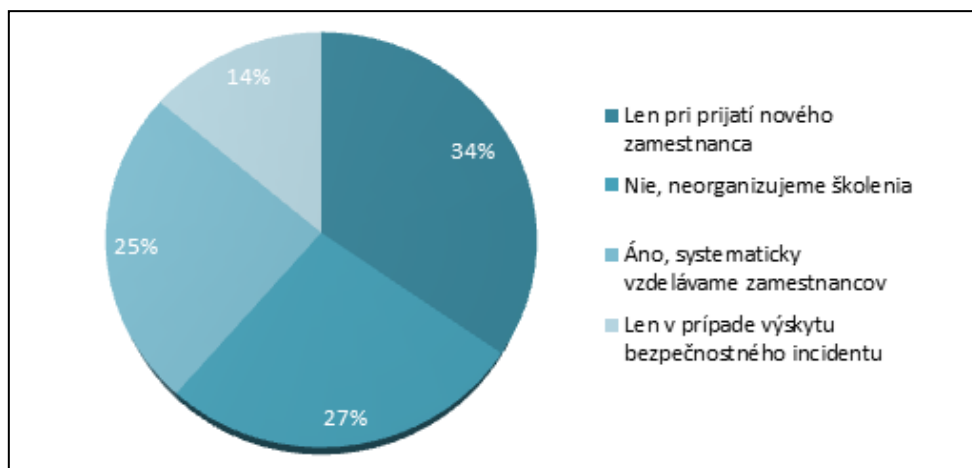
Z pohľadu útočníka je oklamanie zamestnancov omnoho menej náročné a namáhavé ako prekonanie niekoľko faktorovej sieťovej ochrany. Úspešnosť útokov závisí od ľudskej chyby, nepozornosti, nedbalosti, nevedomosti, či dokonca hlúposti. A skutočne sfaľovať e-mail, do ktorého je vložený škodlivý kód, ktorý pri troche šťastia obeť aj sama „nečujne“ aktivuje, prípadne využitie podvodnej webovej stránky, pdf dokumentu, alebo obľúbenej sociálnej siete je oveľa menej namáhajúce, ako prekonať firewall, IDS, či IPS systém, rôzne autentifikačné nástroje a ešte k tomu aj zahladať po sebe stopy. Sociálne inžinierstvo je efektívnejšie aj z pohľadu času a financií. Útočník môže viac času venovať napríklad programovaniu špionážneho kódu, ako prekonávaniu obranných prostriedkov danej siete.

Ponúka sa stále aktuálny výrok pripisovaný Einsteinovi: „Na svete sú iba dve veci nekonečné: vesmír a ľudská hlúposť. Aj keď tým prvým si nie som celkom istý.“ To podporuje aj zistenie z prieskumu stavu informačnej bezpečnosti v organizáciách na Slovensku z roku 2011, organizovaného spoločnosťou ESET. V ňom 63 percent organizácií označilo za príčinu výskytu bezpečnostného incidentu správanie zamestnancov. Táto skutočnosť môže súvisieť s úrovňou vzdelávania a budovania bezpečnostného povedomia v organizácii. Z prieskumu tiež vyplýva, že len 25 % organizácií organizuje pravidelné školenia v oblasti informačnej bezpečnosti. Ostatných 75 % školí zamestnancov v oblasti bezpečnosti iba jednorazovo (pri nástupe do zamestnania alebo po výskyte bezpečnostného incidentu) alebo ich neškolí vôbec. [5]



Graf 1: Dôvody výskytu bezpečnostného incidentu v organizáciách

Prameň: [5]



Graf 2: Budovanie bezpečnostného povedomia prostredníctvom školení o IB

Prameň: [5]

Útočník musí:

- byť presvedčivý,
- budiť dojem dôveryhodnosti (vyjadrovanie, oblečenie, profesionálne vystupovanie, adekvátne vybavenie, ... odpovedajúce falošnej identite),
- mať originálny nápad,
- absolvovať prípravu predchádzajúcu samotnému útoku, ktorej cieľom je o napadnutom subjekte zistiť všetky dostupné informácie, aj návyky,
- oboznámiť sa s pomermi v napadnutej organizácii.

K najpoužívanejším technikám útokov patria:

- falošné webové stránky,
- falošné e-maily,
- falošné telefonáty,
- prehľadávanie odpadu, spracovanie nezlikvidovaných a neskartovaných informácií,
- manipulácia s prenosnými médiami,
- reverzné sociálne inžinierstvo, fyzický vstup do priestorov, falošná identita,
- masový útok cez sociálne siete.

Falošné webové stránky

Na webe je umiestnená ponuka na benefit spojený s prihlásením sa a zadaním hesla (napríklad rýchlejšie sťahovanie zo servera, sprístupnenie novej verzie obľúbenej hry a pod.). Obeť vyplní údaje v presvedčení, že nič neriskuje, ale neuvedomuje si, že použije heslo, ktoré používa na mnohých miestach, aj pri vstupe do firemného systému, či elektronickej pošty.

Falošné e-maily

Jedným z dôležitých prvkov, bez ktorých nie je zväčša možné uspieť, je sfalšovanie adresy odosielateľa. Nejde o zložitý proces, preto sme ho ukážkovo použili aj v rámci vyučovania. Útočník sa môže vydávať za personálnu spoločnosť, za kolegu, rodinného príslušníka, veľmi často sa falšujú e-mailové adresy rôznych spoločností, ktoré poskytujú podporu, prípadne adresy oddelení zameraných na technickú podporu. Ak má správa uspieť, musí obsahovať príznačný predmet, napr. ako sme uviedli vyššie v príkladoch: „hľadanie zamestnancov“, „žiadost' o kontrolu dokumentu“, ale niekedy je úspešný aj lákavý reklamný názov. Telo e-mailu musí obsahovať text, prípadne dizajn, ktorý prinúti užívateľa otvoriť prílohu, prípadne kliknúť na odkaz, ktorý obsahuje. Jednou z ciest je veľmi formálny vzhľad, inou priateľský, často až vtieravý ... Útočník dbá aj na zabránenie odhalenia svojej osoby a podvodný e-mail zvyčajne smeruje cez niekoľko proxy serverov.

Falošné telefonáty

Sociálne inžinierstvo cez telefón je známe už z minulosti, napriek mnohým zverejneným prípadom býva často predmetom nevinných vtipov medzi ľuďmi. V minulosti sa nielen týmto spôsobom preslávil vtedajší veľký hacker, dnes bezpečnostný konzultant - Kevin Mitnick. Jeho technika psychologicky presvedčiť akéhokoľvek pracovníka bola dokonalá. A to stihol už do svojich 17 rokov. Stále sa objavujú útoky, kedy sa volajúci, vydávajúci sa za zamestnanca, ktorý zabudol heslo, dožaduje na technickej podpore jeho resetovania. Prípadne môže naliehať na udelenie prístupových práv do určitých sektorov (napríklad vydávaním sa za externého spolupracovníka, či dodávateľa). Záleží len na pracovníkovi podpory, či sa nechá presvedčiť, alebo sa bude držať protokolu a žiadať všetky patričné autentifikačné náležitosti.

Prehľadávanie odpadu

Z názvu technika nepôsobí príliš sofistikovane, v praxi sa však veľmi často používa. Pre útočníkov sú totiž veľmi cenné aj informácie, ktoré samotní zamestnanci považujú za triviálne. Odhodený telefónny zoznam firmy im poskytne presné tipy na ľudí, na ktorých môžu zamerať útok. Organizačné schémy ich informujú, ako sa volajú vedúci oddelení a kto je koho nadriadeným. Vďaka obežníkom získajú zdanlivo nepodstatné drobné informácie, ktoré im však umožnia, aby ich príbeh pôsobil autenticky. Inštrukcie a manuály im prezradia, aké kvalitné sú bezpečnostné opatrenia. Fantastickým zdrojom informácií sú odhodené kalendáre a poznámky s termínmi stretnutí: dá sa z nich zistiť, ktorí zamestnanci budú v určitom čase mimo kancelárie.

Samostatnou kategóriu sú odhodené a napohľad nefunkčné disky či hardware, z ktorých často možno získať množstvo cenných dokumentov.

Kuriozita z reálneho sveta: spoločnosť Oracle bola pred pár rokmi obvinená z profesionálnej priemyselnej špionáže, keď sa pokúšala prostredníctvom detektívnej kancelárie odkúpiť odpad z budov Microsoftu. [4]

Reverzné sociálne inžinierstvo

Ide o pokročilú techniku, pri ktorej samotní zamestnanci napadnutej firmy požiadajú útočníka, aby im pomohol vyriešiť problém s počítačovým systémom, ktorý útočník sám spôsobil a dobrovoľne mu prezradia požadované informácie.

Prvým krokom je sabotáž: útočník spôsobí v systéme firmy problém. V druhej fáze útočník ponúka vlastné služby tak, aby ho zamestnanci kontaktovali a požiadali o pomoc. Následne prichádza fyzicky do firmy v úlohe legitímneho administrátora či technika, od zamestnancov získa potrebné informácie, skutočne odstráni pôvodný problém, čím aspoň na čas po sebe zahradí stopy.

Masový útok cez sociálne siete

Sociálne inžinierstvo sa dá realizovať i vo vyššej miere ako útokom na jednotlivca, či špecifickú organizáciu. Príkladom je napríklad červ Trojan.FakeAV.LVT šírený prostredníctvom Facebooku. [2] Po objavení linku od dôveryhodnej osoby z kontaktov naň väčšina ľudí bez obáv a bez rozmýšľania klikla. Po kliknutí na odkaz boli užívatelia presmerovaní na stránku s obsahom malware. Z tejto „Facebook epidémie“ jasne plynie, že sociálne inžinierstvo je ľahko a efektívne využiteľný nástroj pre šírenie červov, či už elektronickou poštou, IM protokolmi, alebo sociálnymi sieťami.

3.3 Fáza realizácie

V úvode tejto fázy, pred samotnou debatou, vyhodnotíme činnosť agentov, žiakom predstavíme použité, prípadne dostupné techniky sociálneho inžinierstva. Vzhľadom k tomu, že nie je cieľom prezradiť, ktoré dvojice budú v debate stáť proti sebe, je potrebné konkrétne zistenia nechať v utajení.

Z našich skúseností vyplynulo, že žiaci neboli náchylní prezradiť dôverný obsah, manipulačným technikám teda odolali. V otázke zabezpečenia svojich IT prostriedkov však obozretní, ani podozrievaví neboli takmer vôbec. Žiakovi „agentovi“ sa podarilo dostať k citlivým údajom z prehliadača webových stránok „obetí“, kde z novo pridanej záložky dedukoval náplň činnosti žiakov, v jednom prípade bol úspešný pri „kradnutí“ dát z požičaného USB kľúča. Za najväčší úspech považujeme prienik do schránky elektronickej pošty, kedy agent požiadala spolužiaka o odoslanie riešenia domácej úlohy e-mailom z jeho schránky pod zámienkou nedostatku času priamo na hodine, pričom si preposlal učiteľom zaslané informácie o jeho úlohe v debate.

Čo sa týka phishingu, podľa očakávania na mail odpovedali všetci žiaci, vrátane odoslania požadovaných dát, bez akéhokolvek overovania. Táto úvodná aktivita výborne pripravila atmosféru v skupine na realizáciu prvého debatného kola.

Moderovaná debata by mala presne stanovené pravidlá, s ktorými boli žiaci vopred oboznámení:

1. Učiteľ vystupuje v role moderátora, je nestranný a nevyjadruje svoj názor k žiadnemu príspevku.
2. Každá dvojica má na debatu stanovený čas 20 minút.
3. Moderátor otvára debatu predstavením kauzy a formuláciou tézy.

4. Prvý s príspevkom vystúpi „odporca“, ktorý predstaví pridelené internetové služby v pozitívnom svetle.
5. Počas diskusie nie je priestor na rozsiahle prejavy. V prípade dlhého monológu debatéra zasiahne moderátor, a odovzdá slovo protivníkovi.
6. Po uplynutí časového limitu na debatu nasleduje 10 - minútová diskusia.
7. Po zodpovedaní na otázky spolužiakov je moderátorom diskusia ukončená a nasleduje hlasovanie nedebatujúcich prítomných spolužiakov.
8. Výsledky hlasovania nemajú vplyv na následné hodnotenie výkonu žiakov.

Úlohy učiteľa pri vedení produktívnej moderovanej debaty:

- zabezpečiť, aby každý dostal možnosť hovoriť, aby boli dodržiavané pravidlá hry a aby sa debata netočila stále dookola
- viesť, triediť, sumarizovať, no v žiadnom prípade nevyjadrovať svoje stanovisko,
- ponoriť sa do témy, byť na ňu odborne pripravený,
- konštruktívne smerovať debatu a zaistiť, aby boli prebraté všetky aspekty,
- udržiavať diskusiu v chode, mať pripravené otázky, ak debata nemá spád,
- byť stručný, nerobiť dlhé vyhlásenia,
- klásť vždy len jednu otázku,
- držať sa jednej témy,
- prerušovať dlhé monológy aj napriek tomu, že platí, že človeku by malo byť umožnené dokončiť svoju reč,
- pozorne počúvať, otázkami nadväzovať na výpovede debatérov,
- povzbudzovať, prípadne vyzývať tichých, zdržanlivých účastníkov v následnej diskusii k zapojeniu sa, k prejavu názoru,
- udržiavať debatu v pokoji, hoci každú hádku nemusí hneď prerušiť, v správnom čase upokojiť účastníkov zhrnutím výsledkov, navrhnutím kompromisov, či vyjasnením nedorozumení.

V podmienkach našej školy sme na realizáciu debatných kôl vyčlenili tri „dvojhodinovky“, každá v trvaní 90 minút, v týždňových intervaloch. Na prvej hodine sme sa venovali problematike sociálneho inžinierstva, ako je vyššie uvedené. Následne prebehlo prvé debatné kolo. Na ďalších dvoch „dvojhodinovkách“ vždy prebehli dve debatné kolá. Témy boli diskutované v poradí, v akom sú uvedené v tomto dokumente. Na konci každej dvojhodinovky učiteľ vyhodnotil prácu žiakov, v našom prípade bola súčasťou hodnotenia klasifikácia, do hodnotenia bola zahrnutá aj fáza prípravy. Ako bolo uvedené vyššie, výsledky žiackeho hlasovania nemali vplyv na hodnotenie.

Vzhľadom k tomu, že v danej triede šlo o prvý kontakt žiakov s moderovanou debatou, v mnohých prípadoch aj s diskusnou metódou ako takou, forma práce priniesla výrazný motivačný efekt. Na druhej strane však žiakom chýbali argumentačné zručnosti, sústredili sa skôr na prezentáciu, nenadväzovali v príspevkoch na vystúpenie protivníka. Do debaty sa neorganizovane snažili okrem debatérov zapájať aj ostatní členovia

skupiny, hlavne v prvých kolách. Tu musí jednoznačne sledovať dodržiavanie pravidiel moderátor. Mnohokrát následná diskusia mala väčší emotívny náboj, niektoré reakcie v diskusii boli mierené proti konkrétnemu debatérovi, v prípade prehnaných príspevkov bolo potrebné žiakom vysvetliť, že nejde o konkurenčné prostredie, naopak sledujeme spoločný cieľ a debatéri nie nutne obhajujú vlastný postoj.

4 VÝSLEDKY MODEROVANEJ DEBATY

V tejto kapitole predstavíme žiacke príspevky z jednotlivých debatných kôl. Podkladom je materiál, ktorý žiaci odovzdali v rámci konzultácií. Ten je obohatený o naše poznámky zaznamenané pri moderovaní. Ku každej téme, a jej priradenej kauze a téze, predstavíme najskôr materiál nesúhlasnej strany, teda strany „odporcu“, ktorý v súlade s pravidlami moderovanej debaty dostal ako prvý priestor na vystúpenie. Ďalej materiál súhlasnej strany, teda strany „zástancu“. Každú tému uzavrieme výsledkami hlasovania z našej realizácie debatných kôl, ktoré prekvapivo neskončilo vždy podľa všeobecného očakávania.

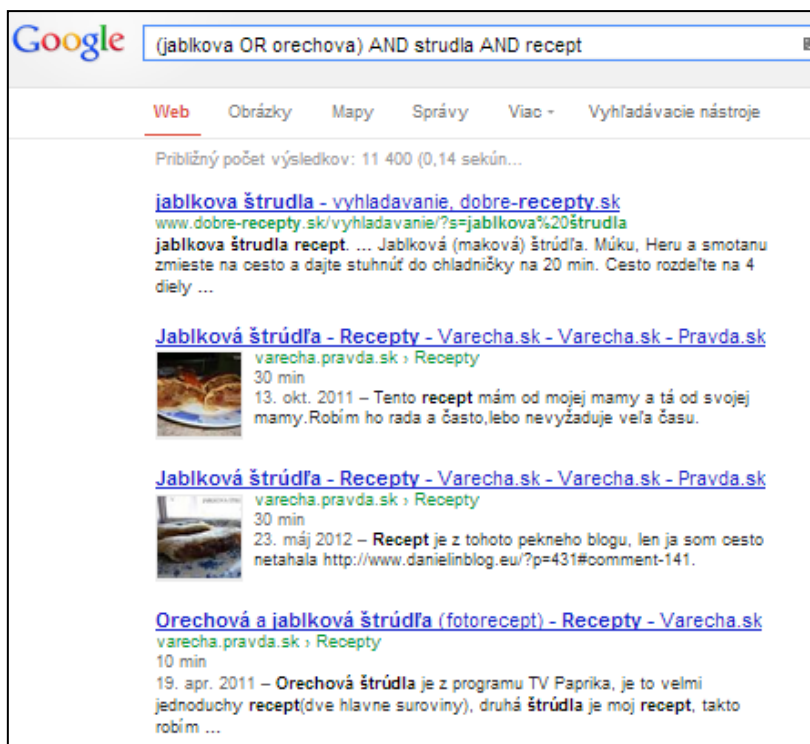
4.1 Publikovanie a vyhľadávanie informácií na webe

Téza: „Sledovanie užívateľskej činnosti na webe by malo byť zakázané.“

Predstavenie služieb odporcom:

- Webový prehliadač je program, ktorý sa používa na prehľadávanie webových stránok v službe www. Služba pracuje na princípe klient – server.
- Vyhľadávanie na internete
 - Katalógy (directories) - zoznamy odkazov na webové stránky usporiadané podľa kategórií hierarchicky, informácie sú schvaľované redaktormi, odkazy na svoje webové stránky môžu pridávať aj ich autori.
Príklady katalógov: Atlas.sk, Zoznam.sk, Centrum.sk, Google-directory
 - Vyhľadávače (search engines) - používajú špeciálne programy na získanie a zaznamenanie informácií o webových stránkach, prvým programom je vyhľadávací robot, ten prechádza záznamami webových stránok, ďalší program ich zaznamená do databázy, ďalší robot ich na základe dopytu ponúkne užívateľovi.
Príklady vyhľadávačov: Google, Morfeo, Live search
 - Metavyhľadávače - nemajú vlastnú databázu, využívajú databázy viacerých vyhľadávačov, výhodou je, že prostredníctvom jedného rozhrania sa dá prehľadať väčší webový priestor.
Príklady metavyhľadávačov: Clusty, Dogpile, All4one
- Spôsoby zadávania vyhľadávacích dopytov
 - Jednoduché dopyty - zadávame priamo do vyhľadávacieho textového poľa, ak zadáme viac slov oddelených medzerou, vyhľadávač hľadá výsledky, v ktorých sa vyskytnú všetky tieto slová. Ak použijeme úvodzovky, chceme aby sa vyhľadalo práve takéto slovné spojenie.
 - Dopyty s operátormi (obr. 1)
(-) Slová, ktoré sa nemajú vyhľadávať
(+) Slová, ktoré nechceme vylúčiť z vyhľadávania
Logické operátory: AND (a zároveň), OR (alebo), NOT (nie).
Prioritu stanovujú zátvorky.
 - Pokročilé vyhľadávanie – pomocou rozšírených nastavení vo vyhľadávači môžeme spresniť dopyt vymedzením jazyka, lokality, veku webovej stránky, formátu súborov, kontroly preklepov, ...
- Špecializované vyhľadávanie
 - Odborovo zamerané katalógy (Math forum, Študovňa google)
 - Encyklopédie, slovníky, weby odborných časopisov

- Portály škôl, univerzít, inštitúcií
- Wiki – systémy (Wikipédia)
- Publikovanie prostredníctvom blogu
 - Je to online internetový denník jednej konkrétnej osoby, ktorý je určený aj pre ostatných ľudí. Skladá sa z článkov, ktoré autor blogu publikuje.
 - Ku každému článku môže byť diskusia.



Obrázok 1 Výsledky vyhľadávania pri použití dopytu s operátormi

Prameň: zdroj autora

Argumenty odporcu tézy:

1. Uchovávanie záznamov o vyhľadávaných informáciách je pre užívateľa prospešné, lebo má ciele poskytnuté informácie, ktoré ho zaujímajú. To mu šetrí čas pri vyhľadávaní. (Praktická ukážka: vyhľadanie lokality na školský výlet na mape, vzápätí sa ponúkajú možnosti ubytovania, stravovacích a rekreačných služieb v okolí.)
2. S reklamou sa človek stretáva denne, v cielej reklame nie je rozdiel, človek má vždy možnosť ignorovať ju.
3. Existujú nástroje typu „Do not track“, ktorých implementácia do prehliadača znemožní zber akýchkoľvek údajov. (<http://donottrack.us/>)

Argumenty zástancu tézy:

1. Sledovanie internetovej činnosti, vrátane lokalizácie, kontaktov, vyhľadávacích dopytov, komunikácie, záujmov je porušovanie súkromia
(<http://earchiv.chip.cz/cs/earchiv/rubriky/internet-archiv/kdo-surfuje-s-vami.html>)

2. Sledovanie je nebezpečné nielen v prípade ilegálnej činnosti: hrozí SPAM, phishing, agenti ponúkajúci svoje výrobky – tým sa bežný človek nie vždy vie brániť.
3. Návštevníci webu sú neprávom značkovaní cez „cookies“ aj na desiatky rokov, za taký čas sa človek môže zmeniť, a údaje môžu byť zneužitú v jeho neprospech.

Cookies - užívateľov označujú pomocou „Session-ID“ – dočasné cookies, ešte behom „prechádzky“ internetových obchodov dokážu predložiť rôzne ponuky tovaru, ktoré užívateľ najviac prezeral, dáta cookies sú ukladané na dobu desiatok rokov, aby uchovávali všetko o zvykoch a záľubách zákazníkov, pod rúškom pomoci pri automatickom vyplňaní evidujú aj citlivé údaje o užívateľovi, ktoré sú ľahko zneužitelné formou sociálneho inžinierstva.

Riešenie:

- zakázať automatické spracovanie cookies -> potvrdzovať na každej stránke prijatie cookies (zdĺhavé)
 - pravidelne vymazávať cookies
 - používať „anticoookie“ software (pohodlné, ale čo ak nie je spoľahlivý?), ktorý mení priebežne identity užívateľa a zahľcuje prevádzkovateľa veľkým množstvom nezaraditeľných údajov.
(<http://www.cookiecentral.com/ccstory/cc5.htm>)
4. Google pri prihlásení v jednej službe sumarizuje údaje aj o všetkých iných využívaných službách. Riešenie: Odhlasovať sa pri vyhľadávaní z google účtu.

Výsledky hlasovania: zvíťazil zástanca.

4.2 Ukladanie, prenos a zdieľanie údajov

Téza: „Cloudové úložiská sú centrá počítačového pirátstva a napomáhajú plagiátorstvu.“

Predstavenie služieb odporcom:

- Prenos súborov je jedna z najzákladnejších sieťových služieb.
- FTP - súbory sú uložené na počítači, ktorý sa volá File server, ten ich poskytuje klientom na ich vlastnú žiadosť (download), resp. môže klient odoslať súbor na FTP server (upload).
- Dátová úschovňa - ak potrebujeme preniesť veľké množstvo dát, môžeme použiť špeciálne dátové úložisko, systém súbor preniesie na server a upozorní určeného príjemcu automaticky odoslanou správou na uvedený mail, tá informuje o podmienkach uloženia zásielky. (<http://www.uschovna.cz>)
- Cloudové úložisko - poskytovanie diskového priestoru na ukladanie dát, dostupné prostredníctvom internetu kedykoľvek, kdekoľvek. (<https://www.dropbox.com/>, <http://www.ulozto.cz/>)
- Cloud computing - poskytovanie služieb alebo programov uložených na serveroch niekde na internete s tým, že používatelia k nim môžu pristupovať napríklad pomocou webového prehliadača a používať ich prakticky odkiaľkoľvek. Rozšírenie vyššie uvedenej služby. Umožňuje nastavenie pravidiel zdieľania súborov a spoločný prístup k súborom a aplikáciám – výhoda pri tímovej práci. (<https://drive.google.com/>)

- Streaming - technológia prehrávania audia a videa v reálnom čase (napr. on-line TV vysielanie, počúvanie rádia a pod.) (<http://www.funradio.sk/stream/>)
- Podcast - zvukové alebo video záznamy, ktoré autor podcastu umiestňuje na internet v podobe súborov, na ktoré odkazuje na webových stránkach. (<http://www.youtube.com>)

Argumenty odporcu tézy:

1. Úložiská sú prevratnou technológiou, vďaka ktorej majú užívatelia k dispozícii diskový priestor na ukladanie multimédií.
2. Použitím šifrovania je zaručená bezpečnosť informácií.
3. Počítačové pirátstvo je súčasťou internetu, nezanikne zrušením, či zákazom cloudových technológií.
4. Proti porušovaniu autorských práv môžu bojovať sami autori, portály sprísnil bezpečnosť a dali vyššie právomoci autorom. (<http://byznys.ihned.cz/c1-54748100-uloz-to-vyslyselo-stiznosti-autoru-zvysuje-zabezpeceni-proti-zneuzivani-serveru>)
5. Plagiátorstvu záverečných prác bráni Centrálny register záverečných prác. (<http://www.crzp.sk/>)

Obrázok 2 Centrálny register záverečných prác (<http://www.crzp.sk>)

Prameň: zdroj autora

Argumenty zástancu tézy:

1. Zriaďovanie cloudových úložísk podporuje ukladanie a voľné šírenie warezu. (<http://www.itnews.sk/spravy/bezpecnost/2013-01-22/c153713-protipiratske-skupiny-chcu-odstrihnut-sluzbu-mega-od-penazi>)
2. Súčasťou warezu je často malware, takže cloudové úložiská podporujú počítačovú kriminalitu. Už aj google zaujal odmietavé stanovisko. (<http://magazin.stahuj.centrum.cz/google-udelal-prvni-krok-proti-warezu/>)

3. Porušovanie autorských práv aj plagiátorstvo prosperuje z dostupnosti pirátskych kópií.
(<http://www.cpuofilm.cz/press.html>, <http://www.itnews.sk/spravy/biznis/2012-08-24/c150630-vplyv-dohody-acta-pokracuje-fbi-vypina-piratske-stranky-s-androidovymi-aplikaciami>)
4. Plagiátorstvo je vďaka úložisk spoločensky tolerované.
(<http://www.sme.sk/c/6385609/plagiator-rozbieha-novu-fakultu.html>)

Výsledky hlasovania: zvíťazil odporca.

4.3 Elektronické kancelárie, pobočky, obchody

Téza: „Nákupom v internetovom obchode vedome podstupujeme riziko podvodu.“

Predstavenie služieb odporcom:

- eGovernment - elektronická forma výkonu verejnej správy pri aplikácii informačno-komunikačných technológií (ďalej IKT) v procesoch verejnej správy. V týchto procesoch funguje on-line komunikácia:
 - v rámci inštitúcií VS (G2E – Government to Employee)
 - medzi inštitúciami VS navzájom (G2G – Government to Government)
 - medzi verejnou správou a občanmi (G2C - Government to Citizen)
 - medzi verejnou správou a podnikateľskou sférou (G2B - Government to Business)
 - medzi verejnou správou a administratívou (G2A - Government to Administration)

Ústredný portál verejnej správy Slovenskej republiky:

<http://portal.gov.sk/Portal/sk/default.aspx>







The screenshot shows the homepage of the central portal of the Slovak Republic's public administration (portal.gov.sk). The header includes the logo and navigation links for 'Kontakt', 'English version', 'O portáli', 'Návod na použitie', and 'Pomoc'. The main content area features a warning message: 'UPOZORNENIE: Pre potreby elektronických služieb, ktoré vyžadujú podpisovanie elektronickým kľúčom si stiahnite nový podpisovací nástroj tu. Pred inštaláciou si prosím prečítajte návod na použitie.' Below this, there are three main sections: 'Občan' (Citizen), 'Životné situácie' (Life situations), 'Agendy' (Agendas), and 'Služby' (Services). The 'Občan' section lists various services like 'Doklady a evidencia', 'Spotrebiteľ', 'Dôchodky, študenti a poistenie', and 'Životné krízy'. The 'Agendy' section lists 'Zákon a právo', 'Daň z nehnuteľností', 'Cestovné doklady', 'Ochrana osobných údajov', 'Evidencia motorových vozidiel', and 'Minimálna mzda'. The 'Služby' section lists 'Katastrálny portál – vyhľadávanie' and 'Podanie na Slovenskú obchodnú inšpekciu'. The sidebar on the right contains a 'Prihlásenie' (Login) section with fields for 'Prihlásenie:' and 'Heslo:', a 'Zapamätat' prihlásenie' checkbox, and a 'Prihlásiť' button. Below the login section are links for 'Zaregistrujte sa', 'Výhody registrácie', and 'Zabudnuté heslo'. At the bottom of the sidebar is a 'Dokumenty a tlačivá' (Documents and forms) section with a link to 'Dokumenty a tlačivá'.

Obrázok 3 Ústredný portál verejnej správy Slovenskej republiky (<http://portal.gov.sk>)
Prameň: zdroj autora

- Portály vzdelávacích inštitúcií
 - oficiálne školské weby informujú návštevníkov o aktualitách z oblasti školstva, základných pedagogických dokumentoch, projektoch, súťažiach, školeniach,
 - weby zamerané na vzdelávanie obsahujú aj stránky s učebnými textami, aktivity pre žiakov, diskusné fóra, videá a pod.
 - Weby školských organizácií a projektov:
 - <http://www.infovek.sk/>
 - <http://www.univerzita.net/>
 - <http://www.iuventa.sk/>
 - <http://www.modernyucitel.sk/>
 - Formy internetového vzdelávania:
 - e-Learning – vzdelávanie, pri ktorom sa využívajú rôzne multimediálne technológie a internet.
(<http://www.e-ducation.com>)
 - On-line vzdelávanie – hlavným prostriedkom na doručovanie obsahu výučby a komunikáciu je internet.
 - LMS – systém pre správu výučby – umožňuje komunikáciu medzi učiteľmi a žiakmi, evidenciu činnosti žiaka, sprístupňovanie učebných materiálov, vrátane oprávnení pre prístup k nim.
(<http://moodle.org/>)
- Elektronické bankovníctvo
 - moderná forma platobného styku, klient neprichádza do osobného kontaktu so zamestnancami banky pri vybavovaní bankových záležitostí, dovolené operácie realizuje prístupom z internetu,
 - komunikácia prostredníctvom moderných telekomunikačných technológií ako je mobilný telefón, internet, fax, či telefón s pevnou linkou. Na identifikáciu klienta slúži tzv. PIN kód, prihlasovacie meno, heslo a GRID karta /plastová karta s číselnými kódmi pre potvrdenie transakcií – slúži ako podpis klienta/.
- Elektronický obchod - internetový obchod alebo e-shop alebo e-obchod alebo online obchod je obchod (resp. aj obchodovanie) na internete. "Opakom" internetového obchodu je najmä klasický, v tejto súvislosti prezývaný "kamenný" obchod.
 - Výhodou internetového obchodu sú spravidla nižšie náklady než v prípade kamenných obchodov, a tým aj nižšie ceny.
 - Nevýhodou sú problémy spojené s bezpečnosťou nákupu a najmä osobných údajov.
 - Spravidla platí, že u známych internetových obchodov je bezpečnosť vysoká.

Argumenty odporcu tézy:

1. Spravidla platí, že u známych internetových obchodov je bezpečnosť vysoká.
2. Hodnotenie internetových obchodov je verejne dostupné u viacerých nezávislých spoločností. (<http://obchody.heureka.sk/>, www.bezpecnynakup.sk/)

	<p>HEJ.sk Najväčšie obchodné internetové centrum v SR - HEJ.sk. Na stránkach HEJ.sk môžete nájsť širokú ponuku audio-video, fotoaparátov, mobilných telefónov, bielej techniky, auto-moto potrieb, PC produktov, športových potrieb,...</p> <p>www.hej.sk</p>	 20008 recenzií
	<p>Alza.sk Alza.sk je slovenské zastúpenie najväčšieho českého internetového obchodu s počítačmi a elektronikou Alza.cz. Ponúkame Vám nadštandardné služby, na ktoré sa môžete spoľahnúť. Nákup u nás je jednoduchý a bezpečný....</p> <p>www.alza.sk</p>	 4382 recenzií
	<p>MALL.sk Na trhu už od roku 2005. Okrem elektroniky a domácich spotrebičov nájdete u nás aj športové vybavenie, hobby potreby, kosačky, bicykle, hodinky, parfémy, značkové oblečenie, plienky, krmivo pre psov, drogériu a ďalšie....</p> <p>www.mall.sk</p>	 19183 recenzií
	<p>talkive www.talkive.sk</p>	 6519 recenzií
	<p>Shoppie.sk Shoppie.sk je nový internetový obchod s elektronikou, ktorý vám prináša nový zážitok z nakupovania. Môžete si vybrať zo širokej ponuky elektroniky, najmä domáce spotrebiče, LCD a plazmové televízory, digitálne...</p> <p>www.shoppie.sk</p>	 6055 recenzií

Obrázok 4 Hodnotenie internetových obchodov (<http://obchody.heureka.sk>)

Prameň: zdroj autora

Argumenty zástancu tézy:

1. Každý má možnosť zakúpiť tovar v kamennej predajni, takže keď si vyberie internetový obchod, kde sú nižšie ceny, musí rátať s občasnými podvodmi.
2. Výhodné ceny sú relatívne, lebo predajca o nás zbiera informácie, na základe ktorých na nás cieľi reklamu, ktorej keď podľahneme, prideme o pôvodne usparené peniaze.

(<http://www.chip.cz/clanky/internet/2010/11/clanky/internet/2010/05/nakupovani-na-miru>)

Výsledky hlasovania: zvíťazil odporca.

4.4 Komunikačné služby

Téza: „Diagnóza závislosti od internetu nie je odborné uznaná, problém je zveličený, psychicky zdravých ľudí neohrozuje.“

Predstavenie služieb odporcom:

- Počítačom sprostredkovaná komunikácia (CMC - Computer Mediated Communication) - akákoľvek forma interakcie ľudí prostredníctvom dvoch alebo viacerých počítačov zapojených v sieti.
- Komunikačné služby sa delia na interaktívne, neinteraktívne a špeciálnu kategóriu tvoria sociálne siete.

- Pri komunikácii musíme dbať na dodržiavanie NETIKETY (všeobecne uznané pravidlá pri práci na internete).
- Komunikačné aplikácie
 - lokálne: nainštalované na lokálnom počítači, spustiteľné v ľubovoľnom čase
 - dostupné cez webové rozhranie: poskytuje rovnaké alebo aspoň základné nástroje lokálnej aplikácie
 - prenosné: nevyžadujú inštaláciu a môžu byť uložené na prenosnom pamäťovom médiu.
- Interaktívne komunikačné služby – užívatelia si bezprostredne vymieňajú informácie a okamžite reagujú jeden na druhého (sú online).
 - Zasielanie okamžitých správ: forma komunikácie medzi dvoma alebo viacerými ľuďmi založená na posielaní krátkych textových správ. Umožňuje:
 - odoslanie správy osobe z našich kontaktov,
 - odpoveď na správu,
 - odoslanie skupinových správ,
 - uskutočnenie hlasovej komunikácie,
 - prenášať video z pripojenej kamery,
 - zaznamenať konverzáciu,
 - posielat' súbory,
 - hrať sieťové hry a podobne.
 - Chat: podobný ako zasielanie okamžitých správ, rozdiel: diskutujúci sú pripojení vo virtuálnej miestnosti (chat room).
 - Chat room: má určenú tému rozhovoru, pravidlá, niekedy aj moderátora (umožňuje vstup účastníkom, no má pravo aj vykázat' ich).
 - Hlasový chat: komunikácia prebieha vzájomnou výmenou hlasových správ
 - Videokonferencia: slúži na vzdialenú interaktívnu komunikáciu medzi dvoma a viacerými účastníkmi, ktorí sa navzájom počujú a vidia vďaka prenosu zvukových a obrazových dát cez internet.
 - Videokonferenčné programy (prenos obrazu a zvuku): okrem videokonferencie, umožňujú aj posielanie textových správ a súborov, zdieľanie aplikácií, zálohovanie konferenčných hovorov. Používané programy: MS NetMeeting, MSN Web Messenger, Yahoo Messenger, Skype.
 - Dátová konferencia - spojenie dvoch alebo viacerých účastníkov s cieľom zdieľať dáta.
 - výstupné zariadenia (tlačiareň, obrazovka) môžu byť zdieľané,
 - vstupné zariadenia (klávesnica, kamera) môžu byť použité na ovládanie iného počítača.
 - výhodné na inštaláciu a prácu na vzdialenom počítači, upravovanie chybných dát, zdieľanie prezentácií a podobne.
 - IP telefonovanie: umožňuje prenos zdigitalizovaného hlasu prostredníctvom počítačovej siete alebo iného média prístupného pre protokol IP.
 - Koncové zariadenie: hardvérový IP telefón alebo softvérový IP (aplikácia bežiaci na lokálnom počítači)

- Neinteraktívne komunikačné služby - užívatelia nemusia okamžite reagovať (môžu byť offline). Teda informácie, ktoré sú vyslané jednou osobou sa k adresátovi dostanú po istom čase a ten na ne reaguje s istým časovým odstupom.
 - Elektronická pošta (e-mail): komunikácia prebieha prostredníctvom správ, ktoré si používatelia posielajú.
 - Na jednej strane je používateľ – poštový klient a na strane druhej je poštový server.
 - Poštový server svojim zákazníkom ukladá prijatú poštu do poštových schránok. Používateľ elektronickej pošty musí mať na svojom počítači nainštalovaný program označovaný ako poštový klient.
 - Poštovým klientom môže byť ľubovoľný dostupný program schopný prijímať a odosielať elektronické správy.
 - e-mailovú schránku môže poskytnúť prevádzkovateľ Internetu alebo si ju môžeme založiť sami na niektorom z verejných poštových serverov (www.zoznam.sk, www.post.sk, www.gmail.com, ...).
 - Elektronický distribučný zoznam: špeciálna nadstavba e-mailu, distribúcia informácií pomocou e-mailu množstvu používateľov (zvyčajne automatický systém s obsahom niekoľkých zoznamov). Správy zaslané na adresu systému sú buď interne spracované alebo rozposlané na adresy niektorého zo zoznamov.
 - Internetové fórum: tvoria ho webové aplikácie určené na vzájomnú diskusiu používateľov, obsah je vytvorený používateľmi (nové príspevky, reakcie, vlákna konverzácie...).

Argumenty odporcu tézy:

1. Ľudí so závislosťami nelátkovej povahy celosvetovo pribúda. Pozorovateľné príznaky závislosti:
 - strata kontroly nad časom - postihnutý stráca pojem o čase, ktorý strávil pred monitorom na úkor iných aktivít, ktorým sa rád v minulosti venoval
 - klamanie - postihnutý klame seba i svojim blízkym, čo počas dňa robili alebo koľko času strávil na internete
 - zmena osobnosti - potenciálne postihnutý sa na internete stáva niekým iným ako v skutočnosti je, žije dvojaký život
 - emotívna nestabilita - pocit šťastia, keď si sadnete za počítač a pripojíte sa na internet, strieda pocit viny za čas strávený na internete a zanedbanie tak iných povinností
 - zúfalstvo - postihnutý reaguje podráždene ak z nejakého dôvodu nemôže stráviť ľubovoľný čas na internete
 - fixácia - postihnutý myslí na počítač pri iných aktivitách
2. Prípady zo sveta
 - Dvadsaťročná Chris Staniforthová zo Sheffieldu zomrela v dôsledku komplikácií spôsobených krvnou zrazeninou po 12 hodinách strávených nad internetovou hrou. Jej komplikácie boli podobné žilovej trombóze, ktorou sú ohrození pasažieri dlhých letov.
 - Matka malého dieťaťa bola odsúdená na 25 rokov väzenia, pretože kvôli hodinám stráveným nad hrou na internete nechala svoju dcéru hladovať.

Colleen Christiová bola natoľko zamestnaná hrou World of Warcraft, že si ani nevšimla, že jej dcéra umiera hladom. Trojročné dievčatko, ktoré bolo prevezené do nemocnice v bezvedomí, vážilo iba desať kilogramov.

- Britka Lucienne Maineyová bola odsúdená na 16 mesiacov väzenia za krádež 76 tisíc libier (92 tisíc eur), ktoré potrebovala k financovaniu svojej hráčskej vášne. Na internetové bingo sa dala, keď sa jej rozpadlo manželstvo.

Argumenty zástancu tézy:

1. Uvádzanie prípadov je prvoplánové. Jeho cieľom je šokovať a vystrašiť spoločnosť.
2. Nepoznáme ostatné okolnosti prípadov, psychickú kondíciu ľudí, ktorí podľahli nadmernej internetovej komunikácii.
3. Je pravdepodobné, že títo ľudia by sa stali obeťou inej formy závislosti, keby nemali internet, lebo internetom riešili iné svoje pretrvávajúce problémy.

Výsledky hlasovania: zvíťazil zástanca.

4.5 Sociálna sieť

Téza: „Rozmach sociálnych sietí podporuje rozmach sociálnych deviácií a kyberkriminality.“



Obrázok 5 Reklama na sociálne siete

Prameň: <http://www.videomarketing.sk/socialna-siet.html>



Obrázok 6 Obálka publikácie: Aplikovaná sociálna patológia v sociálnej práci

Prameň: <http://www.prohuman.sk>

Predstavenie služieb odporcom:

- Sociálna sieť je webová stránka určená na nadväzovanie a udržiavanie kontaktov medzi ľuďmi.
 - Sociálne siete môžu byť orientované súkromne alebo pracovne.
 - Každý používateľ si vytvorí vlastný profil, v ktorom napíše o sebe základné informácie.
 - Na základe týchto informácií sa nadväzujú vzťahy medzi používateľmi, ktorí sa spájajú do skupín.
 - Vzájomnými prepojeniami používateľov a skupín vzniká sieť vzťahov, ktoré sú veľmi dôležité v praxi.
 - Prostredníctvom siete užívateľ môže publikovať vlastný obsah – multimediálny, textový, výpovede, názory, postoje.
- Príklady sociálnych sietí:
 - Facebook
 - MySpace
 - LinkedIn
 - Twitter

Argumenty odporcu tézy:

1. Sociálna sieť spája ľudí na celom svete, dáva im možnosť komunikovať, zdieľať životné zážitky a okamihy.

2. Sociálna sieť je prospešný nástroj rýchlej, pohodlnej komunikácie, ktorá uľahčuje množstvo aktivít a povinností.
3. Sociálna sieť umožňuje kontaktovať známych, ktorí by inak boli ťažko dostupní.
4. Závislosť od sociálnej siete je tak markantná, že používateľ dokáže na základe vlastnej potreby nájsť hladinu, obmedzenie času stráveného pri sociálnej sieti.
5. Vírusy sa šíriť dávno predtým, než boli na svete sociálne siete, a keď zaniknú, budú sa šíriť novými modernejšími cestami.

Argumenty zástancu tézy:

1. Nadmerné trávenie času na sociálnej sieti sa prejavuje zanedbávaním svojich vzťahov, pracovných aj sociálnych povinností, objavujú sa poruchy správania, sústredenia alebo fyzické poruchy. To sú základy pre objavenie sa závažnejších sociálnych deviácií.
2. Prvé prípady novodobých nelátkových závislostí, súvisiacich so sociálnymi sieťami, začali liečiť terapeuti v Odbornom liečebnom ústave psychiatrickom na Prednej Hore. (<http://www.zzz.sk>)
3. Mládež uprednostňuje sociálnu sieť pred prechádzkou, aktívnym športom či odpočinkom. Negatívny vplyv na organizmus je nezanedbateľný.
4. Mládež stráca verbálny kontakt, konverzácie v sieti sú plytké, čím dochádza k strate schopnosti prirodzeného vyjadrovania sa, k nedostatku obvyčajnej socializácie.
5. V niektorých prípadoch si môže jednotlivec vytvoriť dokonca imaginárny svet, nereálny, v spoločnosti neznámych priateľov a neskôr sa snaží prvky tohto sveta preniesť do bežného života.
6. Internet a hlavne surfovanie po sociálnych sieťach mení vzťahy celých rodín. Prestávajú vnímať okolie, blízkych, priateľov a reálny svet. Nevedomky sa ocitnú v sieti virtuálnej reality. (<http://www.nebudobet.cz/?page=netholismus>)
7. Keďže komunikujeme iba prostredníctvom internetu, strácame tak niektoré sociálne zručnosti, city a schopnosti empatie.
8. Michalovčanka Alena spomína na dobrú priateľku Ivetu, ktorá pred pár rokmi uviazla v osídloch sociálnej siete pokec. Namiesto kávy jej ponúkla notebook... „Vždy bola spoločenská, rada chodila vonku, dosiahla významné postavenie vo firme, pre ktorú pracovala z domu, pre podriadených organizovala rôzne akcie... Zrazu sa všetko zmenilo – prestala pracovať, chodiť vonku, zaujímať sa o okolitý svet, nedvíhala telefóny.“ Alene to nedalo a šla ju navštíviť. „Ledva mi otvorila dvere, a už utekala do kuchyne, kde mala na stole notebook. Vedľa nej sedel jej 20-ročný syn, tiež s notebookom. Povedala, že len odpíše a hneď sa mi bude venovať,“ opisuje Alena. V šoku si všimla plnú linku neumytých riadov, keď šla do kúpeľne, kopili sa tam hory špinavého šatstva, v byte bol neporiadok. Z chvíľky sa stala hodina. „Pomedzi písanie mi Iveta vysvetlila, že je v skupine na pokeci, že sú tam ľudia z celého Slovenska a aké je to super. Keď som sa ju snažila zatiahnuť do rozhovoru, ako sa má a prečo nechodí medzi ľudí, akoby ma nepočúvala. S úsmevom mi ponúkla, že mi donesie tretí notebook, aby som si začetovala. Keď som odmietla, ďalej sa venovala internetu. Na moje otázky nereagovala a pomaly si ani nevšimla, kedy som odišla.“ Neskôr sa dozvedela, že kamarátka prišla o prácu, je bez peňazí a vystriedala už pár mužov, s ktorými si písala na pokeci.
9. Facebook rozbil rodinu
Svoje vie o závislosti na internete aj 39-ročná Humenčanka Eva. Pred rokom sa po príchode domov z práce jej manžel ani poriadne nenajedol a už sedel pri

počítači. Najskôr sa vyhováral, že potrebuje riešiť pracovné veci, neskôr už ani nevnímal, keď mu Eva niečo hovorila. „Keď sa raz zabudol odhlásiť, v histórii som našla stránky, na ktoré chodí – na prvom mieste boli facebook a pokec. Keď som sa na to otvorene spýtala, bol agresívny a povedal, že ma do toho nič nie je. Prestal sa venovať mne, domácnosti, deťom, stále bol na počítači.“ Neskôr začal manžel chodiť neskoro z práce, potom prišiel, ale v noci odchádzal a vracal sa stále neskôr. „Napokon chodil domov až ráno, voňal rôznymi parfumami a v jeho aute som našla ženské vlasy. Zistila som jeho pokecový nick a zistila, že si píše s viacerými ženami a pochopila som, že ma podvádza. Podala som žiadosť o rozvod,“ spomína Eva.

Výsledky hlasovania: zvíťazil zástanca.

ZÁVER

Z našich doterajších skúseností z vyučovania informatiky na strednej škole vyplýva, že prvým predpokladom pre aktívne včlenenie žiaka do procesu vzdelávania, je zaujať ho. Z tohto pohľadu je vyučovanie, ktoré sa obsahovo týka internetu, vhodné na uplatnenie metód stimulujúcich tvorivú činnosť žiakov. A to najmä vďaka rôznorodosti oblastí, v ktorých má táto téma uplatnenie, čo poskytuje učiteľovi priestor na motiváciu žiakov s rôznymi záujmami. Prípady, na ktorých je vo vyučovaní postavené použitie metódy moderovanej diskusie sú situované do rôznych oblastí informačnej spoločnosti.

Preukázateľný vplyv na výkon žiaka majú aj dostupné pracovné nástroje. Máme za to, že vyučovanie bez podpory IKT prostriedkov a informačných zdrojov, ktoré sú prirodzenou súčasťou mimoškolského života žiaka, by bolo v rozpore s aktivizujúcimi snahami učiteľa. V súlade s tým opisujeme v ukážkach použitie IKT nástrojov, ktoré považujeme za efektívne pre vyriešenie daných úloh a dosiahnutie vymedzených vzdelávacích cieľov. Uplatnenie aktivizujúcich metód vo vyučovaní však nie je podmienené ich použitím.

V neposlednom rade zdôrazňujeme, že získanie pozornosti žiaka, jeho motivácia a záujem sú len prvým krokom na ceste k aktívnemu učeniu sa. Úlohou učiteľa je ďalej ich v činnostiach na vyučovaní využiť k objavovaniu súvislostí, k snahe o zovšeobecňovanie a logické zdôvodňovanie objavených vzťahov. Tomuto zámeru výrazne napomáha prepojenosť úloh so situáciami a problémami z reálneho sveta, z prostredia, ktoré je žiakovi blízke. Z vlastných skúseností teda odporúčame zaradiť navrhnutú metodiku do vyučovania informatiky na strednej škole.

ZOZNAM BIBLIOGRAFICKÝCH ZDROJOV

1. DŽUGANOVÁ, D. Informačná gramotnosť ako kľúčová kompetencia vzdelávania na slovenských vysokých školách. *ProInflow* [online] [cit. 12. 04. 2013]. Dostupné na: <<http://pro.inflow.cz/informacna-gramotnost-jako-klucova-kompetencia-vzdelavania-na-slovenskych-vysokych-skolach>>. ISSN 1804-2406.
2. <<http://forum.viry.cz/viewtopic.php?f=13&t=114694>> [online] [cit. 12. 04. 2013]
3. <<http://siit.webnoviny.sk/pocitace/phishing-spravne-rozpoznalo-len-7-perce/19478-clanok.html>> [online] [cit. 12. 04. 2013]
4. <<http://tech.sme.sk/c/531257/nietore-techniky-socialneho-inzinierstva.html>> [online] [cit. 10. 04. 2013]
5. <<http://www.eset.com/sk/firmy/services/clanky/socialne-inzinierstvo-ib/>> [online] [cit. 13. 04. 2013]
6. <http://www.essetesro.sk/skSK/Solutions/Vedenie_diskusie.html> [online] [cit. 01. 04. 2013]
7. <<http://www.secit.sk/content/umenie-socialneho-inzinierstva>> [online] [cit. 02. 04. 2013]
8. KORŠŇÁKOVÁ, P. – KOVÁČOVÁ, J. *Národná správa OECD PISA SK 2006*. Bratislava : ŠPÚ, 2007. ISBN 978-80-89225-37-8
9. MAŇÁK, J. – ŠVEC, V. *Výukové metódy*. Brno : Paido, 2003. 219 s. ISBN 80-7315-039-5
10. MANNIOVÁ, J. *Kapitoly z pedagogiky*. Bratislava, 2004. 65 s. ISBN 80-968956-2-1
11. PETLÁK, E. *Pedagogicko-didaktická práca učiteľa*. GRIN Verlag, 2008. 68 s. ISBN 978-3-640-13529-5
12. TUREK, I. *Vplyv globalizácie na vzdelávanie* [online]. In Media4u Magazine, roč. 2008b, č. 2 [cit. 16. novembra 2011]. Dostupné na : <<http://www.media4u.cz/mm022008.pdf>>. ISSN 1214-9187
13. VALIŠOVÁ, A. – KASÍKOVÁ, H. *Pedagogika pro učitele*. 2. vyd. Praha : Grada, 2011. 456 s. ISBN 978-80-247-3357-9