Zásady používania výpočtovej techniky
zakúpenej zo zdrojov Filozofickej fakulty Trnavskej univerzity v Trnave

Filozofická fakulta Trnavskej univerzity v Trnave vydáva Zásady používania informačných technológií (IT) a výpočtovej techniky (VT) za účelom stanovenia jednotného postupu zamestnancov pri používaní technických prostriedkov informačných a kancelárskych technológií.

Filozofická fakulta poskytuje svojím zamestnancom technické prostriedky pre kvalitné vykonávanie ich pracovnej náplne, pričom požaduje od svojich zamestnancov zodpovedajúce znalosti z obsluhy VT a používania programového vybavenia.

Pojmy a termíny

Hardware – technické vybavenie počítača (základná doska, procesor, pamäte, disk....)
Software – programové vybavenie, dáta uložené na záznamových médiách.
Pamäťové médiá - sú pevné disky, diskety, magnetické pásky, CD nosiče, USB kľúče a iné médiá používané na uchovávanie dát v elektronickej forme.
Server – vyhradený počítač siete, poskytuje ostatným počítačom siete svoje technické zariadenie, umožňuje užívateľom prístup k spoločným zdrojom dát, komunikačným prostriedkom a ďalším službám.
Protokol – v počítačovej sieti špecifikácia, ktorá definuje postup a parametre vysielania a prijímania dát.
Správca siete - osoba zodpovedná za profilaktiku a správu počítačovej siete.
Používateľ - každý, kto pracuje v prostredí počítačovej siete, využíva jej zdroje a prostriedky. Pre zabezpečenie riadenia prístupu do siete musí mať v sieti vytvorený účet. Ten obsahuje položky, ako prístupové práva k sieťovým zdrojom, údaje o nastavení hesla, jeho členstvo v užívateľských skupinách a iné.
Pirát (hacker) – nepovolaný používateľ výpočtového systému, obvykle osoba so zlými úmyslami. Takáto osoba má právny štatút zlodeja, so všetkými dôsledkami.
Prihlásenie, **autentifikácia** – vytvorenie spojenia s počítačovou sieťou. Obvykle sa vyžaduje identifikačné meno (Login name) a heslo (password). Niektoré systémy požadujú kartu s magnetickým prúžkom alebo elektronickým čipom (bankomat, mobilný telefón,...). Prísnejšie zabezpečené systémy používajú biometriu – odtlačok palca, snímok tváre alebo očnej dúhovky.
Archivácia – systematická činnosť, smerujúca k trvalej ochrane dôležitých údajov pred znehodnotením. Dáta určené na archiváciu za určité obdobie, zvyčajne po uzavretí mesiaca alebo roka, sa trvalo uložia na neprepisovateľné médium. Zodpovednosť za túto činnosť nesie správca IT. Ak sa pri archivácii použije "komprimovací" program, jeho kópia sa pripojí k archivovaným údajom.
Zálohovanie – vytvorenie kópie údajov pre prípad nepredvídanej situácie znehodnotenia alebo straty. Zálohovanie dát vykonáva pracovník zodpovedný za tieto údaje podľa stupňa dôležitosti týždenne alebo aj denne, na prepisovacie média, do osobitného adresára na lokálnom alebo na sieťovom disku. Zálohovanie sa teda vykonáva s dátami pracovného charakteru.
Vírus – program vytvorený s cieľom modifikovať dáta bez vedomia a vôle používateľa.

Poslanie a pôsobnosť oddelenia informačných systémov

Oddelenie informačných systémov FF TU (ďalej len OIS) je poradenským, informačným, školiacim, servisným a gestorským pracoviskom FF TU pre oblasť výpočtovej techniky a informačných systémov. OIS zabezpečuje potreby a úlohy FF TU v oblasti výpočtovej techniky. Pôsobnosť OIS pokrýva oblasti návrhu, nákupu, preberania, vývoja, inštalácie a údržby výpočtovej techniky a programového vybavenia počítačových sietí a multimediálnej počítačovej techniky pre Filozofickú fakultu a pracoviská fakulty, ako aj oblasť školení a používania výpočtovej techniky. OIS zabezpečuje pripájanie pracovísk do sietí TU v Trnave.

Prevzatie zakúpenej výpočtovej techniky na pracovisko

Zakúpená VT je majetkom FF TU v Trnave aj v prípade, že bola získaná z prostriedkov grantov interných zamestnancov fakulty.
Používateľ výpočtovej techniky svojím podpisom na dohode o hmotnej zodpovednosti potvrdzuje prevzatie zverenej výpočtovej techniky na katedru pri preberaní VT z OIS.
V prípade zapožičania vypĺňa žiadosť o výpožičku s doplnením náležitostí, termínu, účelu a zdôvodnenia žiadosti. Žiadosť podpisuje žiadateľ a tajomník fakulty.
Zverenú VT je možné používať na služobné účely a pri pracovných cestách zamestnancov katedier.

Manipulácia s technickými prostriedkami

1) Prostriedky IT a VT musia byť umiestnené tak, aby vplyvom okolia nedošlo k neúmyselnému poškodeniu alebo poruche zariadenia (pádom pracovnej stanice, poškodeniu teplom, vodou, priamym slnečným svetlom, …).
2) Používateľ **môže** manipulovať s výpočtovou technikou (zapínať, používať, vypínať) len v súlade s inštrukciami výrobcu, resp. dodávateľa zariadenia.
3) Používateľ **smie** používať prostriedky počítačovej siete pri svojej práci takým spôsobom, aby nerušil prácu ostatných spolupracovníkov, ani činnosť iných zariadení pripojených do počítačovej siete.
4) Používateľ chráni svoj užívateľský účet pred zneužitím. Pri odchode od počítača vykoná platné odhlásenie, nezverejňuje svoje heslo ani z dôvodu pokračovania v práci inej osobe.
5) Používateľ **smie** používať len svoj užívateľský účet v rámci svojej pracovnej náplne.
6) Používateľ **nesmie** používať počítač k pokusom o získanie neautorizovaného prístupu do zabezpečených systémov v rámci LAN a Internetu.
7) Používateľ **nesmie** znižovať životnosť pracovných staníc a tlačiarní hrubým zaobchádzaním a ich znečisťovaním.
8) V blízkosti technických zariadení je **zakázané** jesť, piť a fajčiť, ale aj vykonávať iné činnosti hroziace znečistením technických zariadení, resp. znížením ich životnosti alebo spoľahlivosti (vibrácie a podobne).
9) Používateľ **nesmie** vykonávať činnosti, ktoré majú deštruktívny dopad na činnosť komponentov počítačovej siete:
   a) robiť zásahy do pracovných staníc, meniť konfiguráciu a sieťové nastavenia,
   b) pripájať k pracovným staniciam ďalšie technické zariadenia, odpájať technické zariadenia pracovnej stanice, okrem USB kľúčov

c) premiestňovať pracovné stanice,
d) meniť výkon počítača zásahmi do pracovnej frekvencie procesora,
e) manipulovať s ovládacími prvkami pracovnej stanice okrem tých, ktoré sú umiestnené na vonkajšej strane skrinky pracovnej stanice, tlačiarne a krytu monitora (zapínanie, vypínanie a „resetovanie“ počítača a tlačiarne, vkladanie a vyberanie diskiet a CD ROM z mechaník, výmena toneru, ovládanie nastavenia jasu, kontrastu prípadne ďalších prvkov regulujúcich obraz na monitore) a to za podmienok oboznámenia sa s ich ovládaním.

10) Opravy a úpravy výpočtovej techniky môže vykonávať len pracovník OIS, resp. prizvaný kvalifikovaný externý špecialista. Externý špecialista pritom môže zasahovať do pracovnej stanice iba s preukázateľným súhlasom zodpovedného pracovníka OIS.
11) Čistenie povrchu technických zariadení od prachu je v kompetencii používateľa. Vnútorné čistenie zariadení môžu vykonávať len pracovníci OIS, resp. kvalifikovaný externý špecialista pri dodržaní podmienok bodu 9.

Manipulácia s pamäťovými médiami

1) Pamäťové médiá musia byť uložené tak, aby nedošlo k poškodeniu záznamu, predovšetkým nesmú byť vystavované pôsobeniu silného magnetického poľa (v blízkosti mobilného telefónu, reproduktora akustického zariadenia, elektrického transformátora), teplotným extrémom, vlhkosti a prašnosti.
2) Do mechaník prenosných pamäťových médií nesmú byť vkladané znečistené alebo poškodené médiá.
3) Pri zapínaní počítača nesmie byť v disketovej mechanike založená disketa.
4) Pamäťové médiá obsahujúce dôverné údaje, musia byť skladované na bezpečnom mieste (uzamykateľný stôl, skriňa, trezor a podobne).

Základné zásady pre manipuláciu s programovým vybavením

1) Používateľ **môže** na pracovných staniciach používať výlučne len programové vybavenie nainštalované pracovníkmi OIS. Používateľ **nemôže** na pracovnej stanici inštalovať ani odinštalovať žiadne programové vybavenie a tiež nemôže meniť konfiguráciu programového vybavenia s výnimkou zmien, s ktorými bol riadne oboznámený na školení o používaní príslušného programového vybavenia.
2) Používateľ **musí** mať základné znalosti práce so súbormi a adresármi v prostredí operačného systému MS Windows. Vytváranie, premenovanie, mazanie a presúvanie súborov medzi disketou, diskami počítača a počítačovej siete sa predpokladá ako základná požiadavka na splnenie uložených pracovných úloh. Používateľ **musí** vedieť štandardne používať OS MS Windows, lokálne nainštalovaný antivírový program, kancelársky balík MS Office, internetový prehliadač MS Explorer, program pre e-mailovú poštu, poskytnuté programové vybavenie so všetkými zabudovanými službami a špeciálne programy poskytnuté k splneniu konkrétnej pracovnej úlohy.
Používateľ, ktorého pracovné úlohy sú závislé od platnej legislatívy SR, pri svojej práci **musí** sledovať a iniciatívne sa zoznamovať so zmenami v legislatíve. Sám požaduje v čase nadobudnutia platnosti legislatívnej zmeny od OIS aktualizáciu svojho programového vybavenia.
3) Používateľ **nesmie** vytvárať a distribuovať kópie programového vybavenia inštalovaného na pracovnej stanici ani pod zámienkou vytvárania záložných kópií.

4) Je **zakázaný** akýkoľvek zásah do nastavení CMOS pracovnej stanice. Povolený zásah sa netýka prípadnej odôvodnenej zmeny bootovacieho hesla.
5) Používatelia pred opustením pracoviska sú **povinní** ukončiť prácu s programovým vybavením, odhlásiť sa zo siete a z operačného systému a nakoniec pracovnú stanicu vypnúť.
6) Pri krátkodobej neprítomnosti **môže** používateľ, pokiaľ mu to používané programové vybavenie umožňuje, nahradiť odhlásenie sa zo systému a vypnutie pracovnej stanice spustením šetriča obrazovky s heslom.
7) Používateľ je **povinný** vykonávať základnú údržbu pracovnej stanice - vyčistenie povrchu pracovnej stanice, obrazovky monitora, klávesnice. Aspoň raz mesačne odstrániť nepotrebné súbory z adresára Kôš. So spôsobom vykonávania základnej údržby systému sa používatelia oboznámia na školení.
8) Používateľ je **povinný** po inštalácii novej verzie programového vybavenia po dobu minimálne jedného týždňa venovať zvýšenú pozornosť činnosti systému a kontrolovať správnosť výsledkov práce. Prípadné odchýlky od požadovaného stavu je povinný čo najúplnejšie zdokumentovať a bezodkladne ohlásiť pracovníkom OIS.

Prístupové heslá

1) Používateľ je **povinný** svoje prístupové heslá meniť najmenej jedenkrát za určené obdobie, prípadne ihneď na výzvu pracovníka OIS.
2) Prístupové heslá používateľa musia mať aspoň 8 znakov (prístupové heslo šetriča obrazovky aspoň 6 znakov). Pre heslo sa neodporúča používať takú kombináciu znakov, ktorú je možné priradiť k jeho osobe, akými sú napríklad meno používateľa a jeho rodinných príslušníkov, telefónne číslo domov alebo na pracovisko a podobne.
3) Používateľ **musí** svoje prístupové heslo používať tak, aby sa ho nemohla dozvedieť iná osoba, ani pracovníci OIS. Používateľ si musí byť vedomý svojej zodpovednosti za aktivity v systéme, ktoré sa vykonajú pod jeho menom a heslom.
4) V prípade podozrenia, že iná osoba pozná heslo používateľa, je používateľ **povinný** svoje heslo okamžite zmeniť.
5) Používateľ sa prihlasuje do siete a do aplikácie pod svojím menom a svojím heslom aj v prípade, že pracuje na pracovnej stanici pridelenej inému používateľovi.

Manipulácia s údajmi

1) Používateľ, ktorý vytvára a používa súbory uložené na disku pracovnej stanice, je **povinný** ich zálohovať. Na to použije prioritne službu programového vybavenia s ktorým pracuje, ak má program túto službu zahrnutú v menu. So spôsobom zálohovania sa používateľ oboznámi na školení. Za údaje uložené na lokálnom disku nesie zodpovednosť používateľ, ktorý ich vytvoril. Používateľ tieto údaje zálohuje na diskety alebo iné pamäťové média a uskladňuje na bezpečnom mieste (uzamykateľný stôl, skriňa, alebo trezor, kľúče od trezoru nesmú zostať voľne prístupné), alebo ukladá na sieťovom disku. Údaje uložené na sieťovom disku sú automaticky zálohované správcom siete.
2) Používateľ **môže** vytvárať tlačové výstupy len v rozsahu určenom jeho pracovnou náplňou. V prípade výstupov obsahujúcich údaje dôverného charakteru (osobné údaje) musí používateľ zabezpečiť, aby k príslušnej tlačiarni nemala počas tlačenia výstupov nekontrolovaný prístup neoprávnená osoba. Vytlačené výstupy obsahujúce údaje

dôverného charakteru musia byť skladované, resp. zlikvidované tak, aby nedošlo k narušeniu ich dôvernosti.

3) Používateľ **nesmie** poskytovať informácie dôverného charakteru nepovolaným osobám v zmysle zákona č.428/2002 Z.z. o ochrane osobných údajov.
4) Používateľ **môže** poskytovať údaje z informačnej sústavy externým subjektom len v rozsahu určenom jeho pracovnou náplňou a ďalšími predpismi. Výnimku tvoria údaje už zverejnené alebo určené na zverejnenie.

Antivírusové opatrenia

1) Každý počítač musí byť vybavený antivírovým programom. Tieto programy musia byť pravidelne aktualizované.
2) Ak sa na pracovnej ploche používateľa zobrazí varovanie antivírusového programu, že sa na vloženej diskete, disku alebo elektronickej pošte nachádza vírus, používateľ nesmie toto varovanie ignorovať. Za žiadnych okolností nesmie pokračovať v práci ale túto skutočnosť bezodkladne oznámi pracovníkovi OIS.
3) V prípade, že infikovaná disketa patrí inému subjektu, používateľ ju viditeľne a výrazne označí ako napadnutú vírusom a odovzdá ju pracovníkovi informatiky. V prítomnosti pracovníka OIS, prípadne po konzultácii s ním vykoná antivírovú „dezinfekciu“ príslušného pamäťového média. So spôsobom vykonania antivírovej kontroly a „dezinfekcie“ sa používateľ oboznámi na školení. V prípade, že nie je možné vykonať antivírovú „dezinfekciu“ diskety okamžite, musí byť táto disketa viditeľne označená ako infikovaná. Po vykonaní antivírovej „dezinfekcie“ označenej diskety, musí byť toto označenie odstránené.
4) V prípade objavenia vírusu v prijatej elektronickej pošte používateľ bezodkladne o tejto udalosti upovedomí pracovníkov OIS, správcu siete, ako aj odosielateľa predmetnej elektronickej pošty. V žiadnom prípade zavírenú elektronickú poštu neposiela inému adresátovi a na svojej pracovnej stanici ju uschová len dočasne a len na žiadosť pracovníka OIS (na účely ďalšej analýzy prieniku vírusu do systémov pracoviska).

Zaznamenávanie a hlásenie problémov s pracovnou stanicou

1) Používateľ pracovnej stanice zaznamená a pracovníkom OIS bezodkladne ohlási každú vnímateľnú odchýlku od bežnej činnosti pracovnej stanice, predovšetkým však nasledovné udalosti:
   a) hlásenia chýb operačného systému a aplikácií, s ktorými používateľ pracuje (presný prepis chybového hlásenia) spolu so stručným popisom situácie (vykonávaných akcií), počas ktorej sa toto hlásenie vyskytlo,
   b) problémy s technickými zariadeniami pracovnej stanice spolu s popisom situácie, počas ktorej k problémom došlo (popis akcií, zadávaných údajov alebo viditeľných javov, ktoré predchádzali, resp. nasledovali výskyt problému).
2) Používateľ pracovnej stanice zaznamená a svojmu nadriadenému a pracovníkom OIS bezodkladne ohlási každú udalosť, ktorá by mohla indikovať porušenie bezpečnosti IT, predovšetkým však nasledovné udalosti:
   a) výskyt vírusu (prepis varovného hlásenia),
   b) únik údajov s informáciou, aké informácie unikli, kam a ako,
   c) odcudzenie médií s údajmi z pracovnej stanice,
   d) odcudzenie technických zariadení pracovnej stanice,
   e) neoprávnený zásah do technických zariadení pracovnej stanice,

f) neoprávnený zásah do programového vybavenia pracovnej stanice (vrátane výskytu nových súborov alebo adresárov na disku pracovnej stanice) alebo do nastavenia jeho parametrov (napr. nastavené zdieľanie disku alebo adresárov pracovnej stanice).

3) Vyššie uvedené zásady platia aj v prípade, že používateľ dočasne používa pracovnú stanicu pridelenú inému používateľovi, v takom prípade naviac informuje aj používateľa, ktorému bola pracovná stanica pridelená.
4) Používateľ informuje pracovníkov OIS a svojho nadriadeného aj v prípade, keď má podozrenie, že súčasný stav umožňuje narušenie bezpečnosti alebo funkčnosti IT. Používatelia sú povinní spolupracovať s pracovníkmi OIS pri objasňovaní príčin výskytu bezpečnostných problémov, aby mohli byť následne vykonané opatrenia, ktoré by zabránili výskytu podobnej situácie.

Súvisiaca legislatíva

Zákon č.383/1997 Z.z. autorský zákon v znení neskorších predpisov
Zákon č.428/2002 Z.z. o ochrane osobných údajov
Zákon č.211/2000 Z.z. o slobodnom prístupe k informáciám

Zásady používania výpočtovej techniky zakúpenej zo zdrojov FF TU v Trnave boli schválené uznesením č. KD 8.2/11.3.2009 dňa 11.3.2009 a týmto dňom nadobúda účinnosť a stáva sa záväzným predpisom na FF TU v Trnave.

Trnava, 11.3.2009

doc. PhDr. Marta Dobrotková, CSc.
Dekanka fakulty