Otázka č. 2: informační etika, šifrování

Ergonomie a hygiena práce s PC

Pracovní místo

Místnost, kde pracujeme s počítačem, by měla být dostatečně osvětlená. Když se používá umělé osvětlení, světlo by mělo být teplé žluté (popř. bílé) a je lepší neužít LED zářivek, jelikož z nich září modré světlo, které tlumí výrobu *melatoninu* (spánkového hormonu). Okna by neměla být ani za monitorem, ani proti němu (tedy za zády uživatele), nejlepší je, když jsou z boku. Též by měla být vybavena roletami, žaluziemi…

Do místnosti by měl proudit čerstvý vzduch a měla by v ní být optimální teplota (22°C – 25°C) a vlhkost (40% - 60%). Rozdíl mezi teplotu na úrovni hlavy a teplotou u nohou by měl být minimální.

Stěny, strop i podlaha místnosti by měly být barevně sladěné (nekombinovat více než 3 barvy). Je vhodné používat žlutou, hnědou, zelenou či modrou. Červená a fialová působí agresivně, proto jsou nevhodné. Černá také není doporučená.

Stůl

Deska stolu by měla být výškově nastavitelná (65cm – 75cm), na povrchu by měla být matná, aby nevrhala nepříjemné a rušivé odlesky. Pod stolem by měl být dostatečný prostor na nohy. Doporučuje se výsuv.

Správné sezení

Židle by měla být ergonomická. Což znamená, že by měla mít výškově a (popř. hloubkově) stavitelnou výšku všeho (sedák, loketní, zádová, hlavová a bederní opěrka). Tvar zádové opěrky by měl ideálně kopírovat tvar páteře, tzn. mít vyboulení v místě bederní páteře, aby jí fungoval jako opora. Opěrky rukou jsou vhodné, protože také fungují jako opora ulevující páteři.

Mělo by se sedět vzpřímeně, tak aby uši, ramena a boky byly v jedné přímce, je tedy špatně naklánět se k monitoru. Monitor má být přímo před hlavou, aby se uživatel nemusel za ním otáčet, a tak zbytečně namáhat krční svaly. Horní příčka monitoru by měla být v úrovni očí, nikdy ne nad ní. Vzdálenost monitoru a uživatele by měla být zhruba na nataženou ruku (50cm – 70cm). Lokty by se měly držet při těle a svírat úhel 90°. Předloktí by mělo být vodorovné s podlahou a ve stejně výšce jako klávesnice s myší. Zápěstí nesmí být vytočené vzhůru.

Nohy by měly v kolenou svírat úhel 90° a chodidla by se měla dotýkat země celá. Neděje-li se tak, je nutné pořídit si podložku na nohy.

Klávesnice a myš by měly být u sebe v tzv. oblasti dosahu (muži 50cm od těla, ženy 44cm). Je vhodné pořídit si ergonomicky tvarovanou klávesnici (různě zahnuté) a podložku na myš

s gelovou opěrkou předloktí. Při psaní pozor na využívání jedné ruky u psaní klávesových zkratek – psaní velkých kláves pomocí shiftu jednou rukou a psaní ctrl + něco jednou rukou atd.

Kompenzační cvičení

Při dlouhém sledování monitoru, zapomíná člověk mrkat a oko ztrácí schopnost akomodace, je tedy dobré jednou za čas podívat se mimo monitor a zaostřovat na různě vzdálené objekty a nechat oči odpočinout.

Dále by se měla udělat každých 10 minut krátká přestávka, kdy se ruce dají pryč z klávesnice, a minimálně jednou za hodinu přestávka delší, kdy je vhodné se zvednout a na chvíli (od 2 minut) se projít a protáhnout. Je dobré dělat cviky, které protáhnout namáhané části těla (ramena, záda…).

Také je vhodné, aby se stejně tolik času, jako se strávilo u počítače, prožilo sportem či jinou dostatečnou fyzickou aktivitou.

Zdravotní rizika

Problémy, které používáním počítače vzniknou, se většinou projeví až po dlouhé době, kdy už jsou povětšinou závažné. Mohou způsobit i dlouhodobé a nevratné následky.

Nejčastější problémy jsou poškození zad, krční páteře, různé bolesti rukou, syndromy tenisového loktu a karpálního tunelu, potíže se zrakem…

Tyto a spousta dalších zdravotní problémy se označují jako poškození z opakovaného namáhání – RSI (repetitive strain/stress injury).

Informační etika a ochrana autorských práv

Informační etika je oblast morálky uplatňovaná při vzniku, šíření, transformaci, ukládání, vyhledávání a využívání informací. Dotýká se tedy všech oblastí, které jsou spojené s prací s informacemi – knihovnictví, informatika, žurnalistika, politika, učitelství…

Začala se formovat během 80. let, poprvé tento termín použil Rafael Cappuro roku 1987. Informační etika není etikou počítačovou, jež řeší vliv počítačů na moderní svět.

Cíle informační etiky je pozitivní působení informací, správné zacházení s informacemi, a naopak prevence špatného zacházení …

Zásady

- Informace by měly být volně šířeny
- Šíření informací by nemělo být nikomu ke škodě či újmě
- Nepravdivá informace není žádoucí a neměla by se šířit
- Měly by vznikat stále nové informace
- Ten, kdo vytvoří informaci, za ni zodpovídá

Zásady jsou v různých formách kodifikovány v zákonících (např. tiskový zákon), mezinárodních smlouvách a profesních kodexech, jež jsou různé pro každou profesi (knihovníci, novináři).

Můžou se dostat navzájem do konfliktu (např. právo na informaci ve vztahu zaměstnavatel - zaměstnanec). A v takových případech se někdy od sebe liší názory etické s legislativními.

Problémy

Problémy se dělí na mikroetického a makroetické. Mikroetické problémy se týkají hlavně jednotlivců a jejich chování a zacházení s informacemi. Jedná se o: downloading, soukromí, copyright, počítačovou kriminalitu, zabezpečení, tajení a falšování informací.

Makroetické problémy se týkají celé společnosti. Nejvíce řešen je dopad informačních technologií na celou společnost.

Ochrana autorských práv

Autorská práva zaručují autorovi výlučná práva k jeho dílu – k ochraně autorských práv se přistupuje, nastane-li neoprávněný zásah do autorských práv, což je např. porušování licenčních smluv, dělání nelegálních kopií a jejich šíření, padělání, vydávání díla za své, neoprávněné sdílení… Stahování, pokud je jen pro vlastní potřebu, trestné není, což neplatí pro počítačové programy, k jejichž používání musí mít uživatel licenční smlouvu. Následky porušení autorských práv jsou různorodé - většinou se jedná o placení peněz (ušlý zisk, zadostiučinění, pokuty) nebo o omluvu. Výchozím pramenem autorského práva a jeho ochrany je autorský zákon (Zákon č. 121/2000 Sb. zákon o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů).

Kyberšikana

Jedná se o používání elektroniky, informačních kanálů a komunikačních přístrojů za účelem poškození jednotlivců či skupin. Jejími projevy jsou nenávistné zprávy (SMS, e-maily), falešné účty zřízené, aby zostudili oběť, rozšiřování očerňujících materiálů (videa, fotky), vydírání využívající komunikační technologie a další. Na rozdíl od normální šikany probíhá kyberšikana jen na úrovni psychické a trvá mnohem déle (nikoliv několik minut, nýbrž klidně i měsíce). Další rozdíl je, že agresorem nebo obětí se může stát kdokoliv. Agresoři často využívají anonymitu, která na internetu panuje, proto si dovolují dělat mnohem ohavnější a zákeřnější věci než v normálním životě. Někdy funguje šikana a kyberšikana společně – agresoři šikanují oběť fyzicky, natočí si to a vyvěsí video na internet. Jedná se samozřejmě vždy o velký problém, proti kterému je hodno zakročit.

Šifrování

Šifrování (jinak kryptografie) slouží k převádění dat do podoby, v níž nejsou čitelné bez speciální znalosti. Šifrovat lze zprávy, soubory i celé disky. Šifrou se rozumí algoritmus, který data (*prostý text*) převede do nečitelné podoby (*šifrový text*). Klíč slouží k zašifrování a dešifrování dat.

Podle počtu klíčů se šifrování dělí do dvou kategorií: symetrické šifrování, kde se používá jeden klíč, a asymetrické, které používá dvojici klíčů – soukromý a veřejný. V současnosti se používá standardu AES u symetrického šifrování a RSA u asymetrického. V obou případech (zvlášť v tom druhém) se dějí složité matematické operace.

Různé způsoby ukrývání zpráv patří pod stenografii. Dnes se jedná např. o skrývání textu do obrázků či souborů s hudbou a videem. V minulých dobách se užívalo třeba neviditelných inkoustů a spousty dalších způsobů.

Typy šifer

V substituční šifře se znaky nahrazují mezi sebou podle určitého klíče. Klasickým zástupcem je Caesarova šifra, v níž je každé písmeno v abecedě posunuto o stejný počet pozic. Dnes je snadno rozluštitelná, jelikož existuje malé množství možných klíčů.

V aditivních šifrách se šifrovaný znak získá sečtením původního znaku a klíče. Zástupci jsou Vigenèrova a Vermanova šifra. Vermanova šifra je jediná šifra, o které bylo dokázáno, že ji nelze rozluštit.

Transpoziční šifra používá změnu pořadí písmen dle určitého pravidla.

Elektronický podpis

Elektronický podpis slouží k ověřování identity původce dat a ověření integrity dat, tj. že data nebyla po odeslání nějak pozměněna. Lze jej užít i pro komunikaci se státní správou (např. elektronické podání daňového přiznání). Podpis je většinou založen na šifrování pomocí RSA.

Princip fungování

Z dokumentu je pomocí hashovací funkce udělán otisk, který je zašifrován pomocí privátního klíče odesílatele. Hashovací funkce funguje tak, že z dat o libovolné velikosti vytvoří krátký řetězec dat, jenž má vždy stejnou délku. Funkce je jednosměrná, z otisku tedy není možné získat data zpět. Dnes se většinou používá standard SHA-2. Příjemce dat dešifruje podpis pomocí veřejného klíče a tento klíč porovná s otiskem přijatých dat. Je-li rozšifrovaný podpis a vlastnoruční otisk stejný, je vše v pořádku.

Certifikační autorita

Certifikační autorita je vydavatelem certifikátů, které obsahují údaje o majiteli elektronického podpisu a jeho veřejný klíč. Ručí tedy za pravdivost údajů toho, kdo používá elektronický podpis. Certifikační autoritou se může stát každý, kdo ví, jak na to. Mnoho firem má vlastní certifikáty pro potřeby vnitrofiremní komunikace. U nás existují tři autority, s jejichž certifikáty lze komunikovat se státní správou: První certifikační autorita, PostSignum a eIdentity.

Zdroje

Ergonomie a hygiena práce s PC

- https://www.bozpinfo.cz/josra/vybrane-aspekty-ergonomie-pri-kancelarske-praci
- https://flek.cz/clanky/dalsi-tipy-a-informace/ergonomie-prace-s-pc-a-zdrave-sezeni-v-kancelari
- https://www.bezpecnostprace.info/pracovni-urazy/ergonomie-pocitacoveho-pracoviste-a-zasady-bezpecnosti-prace-na-pc-aneb-jak-predejit-rsi-syndromu/
- https://www.cnews.cz/zaklady-ergonomie-jak-si-neznicit-zdravi-u-pocitace/

Informační etika

- https://wikisofia.cz/wiki/Informa%C4%8Dn%C3%AD_etika
- https://www.vysokeskoly.cz/maturitniotazky/knihovnictvi/informacni-etika
- https://clanky.rvp.cz/clanek/o/g/14385/INFORMACNI-ETIKA-I-UVOD-A-VYZNAM.html/
- https://clanky.rvp.cz/clanek/c/g/14967/INFORMACNI-ETIKA-II-KODEXY-PRINCIPY-PARADOXY.html/

Ochrana autorských práv

- https://www.jaknainternet.cz/page/1191/autorska-prava/
- http://www.gjo.cz/upload/dokumenty/autorske_pravo.pdf

Kyberšikana

- http://nebudobet.cz/?cat=kybersikana&page=o-kybersikane
- http://www.e-besedy.cz/internetova-bezpecnost/kybersikana.html

Šifrování

- https://algoritmy.net/
- https://cs.wikipedia.org/wiki/Kryptografie
- http://mozektevidi.cz/kryptografie-sifrovani/

Elektronický podpis

- https://cs.wikipedia.org/wiki/Elektronick%C3%BD_podpis
- https://www.jaknainternet.cz/page/1249/elektronicky-podpis/
- https://cs.wikipedia.org/wiki/Kryptografick%C3%A1_ha%C5%A1ovac%C3%AD_funkce