



EURÓPSKA ÚNIA

Európsky sociálny fond
Európsky fond regionálneho rozvoja



OPERAČNÝ PROGRAM
ĽUDSKÉ ZDROJE



Modul 2: Základy práce s počítačom

Bezpečnosť a ochrana zdravia

6 Bezpečnosť a ochrana zdravia

6.1 Ochrana údajov a zariadení

6.1.1 Chápať zásady politiky výberu vhodných hesiel, akými sú: zodpovedajúca dĺžka hesla, striedanie rôznych znakov, neprezerávanie hesla, pravidelná zmena hesla.

Pri ochrane svojich údajov a zariadení najčastejšie používame heslá. Keďže tieto heslá chránia pre nás dôležité údaje a dáta je nevyhnutné, aby sa k nim nedostal nikto okrem nás. Preto existuje niekoľko základných pravidiel pri zostavovaní hesla.

Správne zostavené heslo by malo v ideálnom prípade spĺňať niekoľko základných kritérií:

- **ľahko zapamätateľné** – heslo, ktoré je ťažko zapamätateľné vedie k tomu, že si ho musíme niekde zapísať resp. si ich nechať zapamätať a to je veľmi nebezpečné.
- **dostatočne dlhé** – čím viac znakov v hesle zvolíme t.j. čím bude heslo dlhšie, tým bude útočníkom dlhšie trvať, kým ho prelomia. Odporúča sa dĺžka aspoň 8 znakov.
- **postavené z rôznorodých znakov** – opäť platí zásada, že čím viac rôznorodých znakov (napr. výkričník, podčiarkovník,...) sa bude v hesle vyskytovať, tým bude ťažšie ho prelomiť.
- **neobsahujúce slovníkové slová** – prelomiť heslá vo forme slovníkových slov, t.j. slov zmysluplných, trvá iba niekoľko minút. Preto, ak chcete takéto slová použiť, odporúčame zamieňať niektoré znaky za čísla a pod. napr. slovo cucoriedka môžeme napísať ako CuC()riedk4.

MOŽNOSTI VYTvorenia UNIKÁTNEHO HESLA

Existuje viacero spôsobov, ktoré nám umožnia vytvoriť unikátne heslo.

- Jednou možnosťou je na vytvorenie hesla použiť **počítačový program**. Takto vytvorené heslá sú dostatočne dlhé, obsahujú kombináciu viacerých znakov a určite sú aj unikátne, ale nespĺňajú zásadu ľahkého zapamätania.
- Oveľa lepším spôsobom vytvorenia hesla je **použitie frázy**. Pri tvorbe frázového hesla si zvolíme nejakú vetu alebo frázu, ktorú si ľahko zapamätáme, napr. Tenis hrávam o 18:45 každý deň. Heslo k tejto fráze bude mať potom tvar Tho1845kd – t.j. začiatkové písmená jednotlivých slov a písmen, ktoré sa vo fráze nachádzajú.

Aby sa k vášmu heslu nedostal nikto nepovoláný myslite aj na tieto pravidlá:

- heslo držte v tajnosti,
- pravidelne ho meňte,

- heslá si nezapisujte, ak je to však nevyhnutné záznam poriadne schovajte,
- heslá neposielajte emailom,
- nepoužívajte automatické ukladanie hesiel.

6.1.2 Chápať pojem firewall a vedieť vymedziť jeho účel.

Internet je rozľahlá verejná celosvetová počítačová sieť. Z daného dôvodu je z hľadiska bezpečnosti nanajvýš vhodné použiť prostriedky na akési bezpečnostné oddelenie lokálnej siete od internetu. Využiť môžeme technológie hardvérové alebo softvérové a tak zabrániť neautorizovanému preniknutiu do nášho počítača. Spoločne ich nazývame - **firewall**, fire wall.

Je to podobné ako pri protipožiarnej stene (firewall) v budove. V budove je totiž protipožiarne stena postavená z protipožiarneho materiálu, ktorý má izolovať a chrániť jednu stranu miestnosti pred ohňom zo strany druhej.

Firewall slúži na oddelenie jednej siete od druhej z dôvodov bezpečnosti. Aby nikto bez príslušných práv prístupu nemohol získať prístup k počítačom v lokálnej sieti. Inak povedané firewall kontroluje informácie prichádzajúce z internetu alebo zo siete a následne im podľa nastavení brány firewall prístup k počítaču zablokuje alebo povolí

Hardvérový firewall sa niekedy označuje tiež ako **firewall machine**, softvérový firewall ako firewall code.

6.1.3 Chápať účel pravidelného zálohovania údajov a ich uloženia vo vzdialenej lokalite.

Ľudia už v minulosti zvykli uskladňovať svoje zásoby na viacerých miestach. Bolo zvykom si stavať dokonca sýpky na druhej strane cesty alebo potokov. Takto sa chránili pred stratou celých zásob. No nenaučili sa chrániť svoje údaje v počítači. Jedným z mnohých spôsobov ochrany údajov a dát v počítači je ich **pravidelné zálohovanie**.

Zálohovanie dát je v podstate **vytváranie** kópií dát tzv. **záložných kópií** (klasickým kopírovaním alebo pomocou špecializovaného softvéru), ktoré sa použijú v prípade, že došlo k poškodeniu alebo zničeniu pôvodných dát.

Zálohovanie je najlepšia ochrana voči akýmkoľvek katastrofám. Je nutné si uvedomiť, že pokiaľ sú údaje uložené na počítači, neznamená to, že sú tam na večné veky. Dáta sa dajú pomerne rýchlo zničiť a je dobré ich mať niekde uložené. Najlepšie je vytvárať si záložne kópie a umiestňovať ich niekde na inom mieste - **vo vzdialenej lokalite**. Nestane sa nám to, že ak prideme o počítač (ohň, krádež,...) prideme aj o údaje (zálohovanie dát však nerieši zneužitie odsudzených dát iba stratu).

Veľmi dôležitým faktorom pri zálohovaní dát, ale hlavne dokumentov, je jeho **pravidelnosť**. Napr. ak na nejakom dokumente pracujeme mesiace a zálohy vykonávame raz ročne, je veľká pravdepodobnosť, že pri poškodení počítača môžeme

ľahko o všetky dáta prísť. Ak by sme zálohy vykonávali týždenne, prideme „len“ o týždňovú prácu.

Často sa problém zálohovania dát rieši nasadením záložného počítača. Tento počítač si pravidelne vyžiada od ostatných počítačov údaje a ukladá ich u seba. Veľmi vhodné je takto zálohovať informácie o používateľských účtoch na sieti a základných nastaveniach počítačov. Na komplexné zálohovanie celých diskov je vhodná aplikácia Ghost.

6.1.4 Chápať význam pravidelných aktualizácií rôznych druhov softvéru, akými sú: antivírusový softvér, aplikácie, operačný systém.

Neustále sa objavuje nový škodlivý softvér, ktorý zneužíva nedostatočné zabezpečenie v systéme Windows alebo v iných programoch a snaží sa poškodiť alebo získať prístup k údajom alebo počítaču.

Aktualizácie systému Windows a ďalšie aktualizácie softvéru opravujú tieto nedostatočne zabezpečené miesta krátko po ich zistení. Pod aktualizáciami si môžeme predstaviť softvérové doplnky, ktoré zabráňujú vzniku problémov alebo ich pomáhajú opraviť, zlepšujú funkčnosť počítača a jeho celkové používanie.

Ak aktualizácie nainštalujete neskôr alebo ich nenainštalujete vôbec, počítač môže byť voči týmto ohrozeniam ľahšie zraniteľný. Musíme mať na pamäti, že je dôležité inštalovať nielen aktualizácie systému Windows, ale aj aktualizácie všetkých aplikácií, vrátane antivírusového programu, ktoré máme na našom počítači nainštalované.

Denne vzniká niekoľko desiatok vírusov a mnohé softvérové firmy vyvíjajú antivírusové programy, ktoré by dokázali s týmito vírusmi bojovať.

Takže tak, ako sa vyvíjajú nové vírusy, o „antivírusoch“ by to malo platiť dvojnásobne. Mnohé antivírusové programy poskytujú svojim klientom stálu on-line podporu. Poskytujú im nové verzie, aktualizácie programu, informácie o nových vírusoch, majú svoje podporné centrá.

Spravidla sa dá antivírusový program nastaviť tak, že bude po zadaní užívateľského mena a hesla pravidelne zisťovať prípadnú aktualizáciu. Ak je aktuálnejšia verzia databázy vírusov a metodika ich dezinfekcie k dispozícii, stiahne ju a aktualizuje aj na našom počítači.

Ak nie je náš počítač pripojený do siete, musíme si aktualizáciu antivírusového programu zabezpečiť sami. Môžeme si ju zvyčajne stiahnuť zo stránky a na prenosnom médiu preniesť do nášho počítača.

6.2 Škodlivý softvér (malvér)

6.2.1 Rozumieť pojmu malvér. Rozlišovať rôzne druhy malvéru, akými sú: vírus, červ, trójsky kôň, špehovací softvér (spyware)

S nástupom počítačov a sietí sa objavilo obrovské množstvo bezpečnostných problémov. Ľudia si už dávno zvykli zamykať svoje domy pred zlodejmi, ale nenaučili sa chrániť svoje údaje v počítači. Takéto správanie vyplýva z toho, že bežný používateľ nevidí žiadneho útočníka, a tak sa naivne domnieva, že je v bezpečí. Mylný pocit bezpečia sa stal osudným už mnohým ľuďom a firmám. Niekedy sa dokonca nemusí jednať ani o žiadneho útočníka, ale len o bežného používateľa, ktorý omylom niečo zaklikne. Zo štatistík vyplýva, že viac ako 60 % škôd je spôsobených ľudskou chybou, 35 % škôd je spáchaných úmyselne z vnútornej siete a sotva 5 % sú útoky z vonkajšej siete. Správny administrátor, ktorý chce udržať svoju sieť bezpečnú, musí dobre poznať systém s ktorým pracuje. Pretože aj ten najlepší systém v rukách neinformovaného administrátora je bezcenný.

Zapamätajte si jednu vec: **neexistujú žiadne 100% zabezpečenia**. Vždy existuje nejaký spôsob ako prelomiť ochranu. Ochranu informácií predstavuje zabezpečenie informácií do takej miery, aby k nim mali prístup len povolané osoby. Nesmie dôjsť k ich poškodeniu, prípadne sfaľšovaniu a každú zmenu v ich obsahu je nutné zaznamenať, aby bolo možné vystopovať prípadného útočníka. V prípade, že zistíme porušenie či narušenie bezpečnosti, je potrebné situáciu nahlásiť osobe, ktorá je za bezpečnosť zodpovedná.

MALVÉR

Pojmom **malvér** vo všeobecnosti označujeme každý jeden škodlivý softvér. Môžeme sem zaradiť jednak vírusy, trójske kone,...

Základné druhy malvéru.

Podľa princípu šírenia malvéru ho môžeme rozdeliť na:

- **Vírus** – počítačový vírus je program, ktorý môže infikovať iné programy tým, že k nim pridá vlastnú kópiu. Touto infekciou sa môže vírus šíriť v počítači alebo v sieti tak, že si používatelia infikujú vlastné programy. Každý infikovaný program (súbor) sa stáva nositeľom vírusu a tým sa infekcia šíri. Hneď ako sa spustí program alebo otvorí napadnutý súbor, začne vírus vyvíjať nejakú nepríjemnú alebo škodlivú činnosť. Existujú neškodné vírusy, ktoré sa prejavujú len výpisom upozornení na obrazovku. Iné skupiny vírusov spôsobujú spomalenie alebo zrušenie systému. Najnebezpečnejšie skupiny vírusov odosielajú informácie z počítača či ničia samotné súbory. Existujú vírusy, ktoré ničia celé sektory pevného disku. Niektoré vírusy sa pokúšajú zničiť aj hardvér počítača.
- **Červ** - samostatný program, ktorý sa sám rozširuje rôznymi kanálmi do ďalších počítačov

- **Trójsky kôň** – často krát sa skrývajú v atraktívnych programoch, ktoré si vieme stiahnuť z internetu zadarmo. Samostatný program sa nerozmnožuje, myslíme si, že je užitočný, ale on na pozadí vykonáva škodlivú činnosť

Podľa účinku malvéru ho môžeme rozdeliť na:

- **spyware** – programy, ktoré zisťujú a kradnú citlivé informácie z počítača, a navyše ich bez súhlasu majiteľa počítača odosielajú cudzej osobe. Informácie, ktoré sú takto odcudzené môžu byť rôzne, od zoznamu mailových adries až po heslo do nejakého systému. Najnebezpečnejším typom spywaru je tzv. **keylogger**. Je to program, ktorý sleduje, zaznamenáva a odosiela stláčanie kláves cudzej osobe. Takto sa cudzia osoba môže dostať k našim heslám do emailu, k číslam kreditných kariet a pod.
- **ransomware** (rukojemnícky softvér) – program, ktorý zneprístupní informácie v počítači a vydiera používateľa.
- **adware** – program, ktorý zobrazuje reklamu.
- **dialer** – program, ktorý vytáča audiotextové číslo.
- **backdoor** – otvorí „zadné vrátka“ a umožní útočníkovi získať kontrolu nad počítačom
- **rootkit** – skrýva činnosť iného, väčšinou škodlivého softvéru
- **botnet** – napadnutý počítač sa zapojí do siete ovládaných počítačov, ktoré vykonávajú napr. paralelné výpočty alebo spoločne realizujú masívny útok na niektoré služby

6.2.2 Rozumieť, ako môže škodlivý softvér nakaziť počítač alebo zariadenie.

Spôsobov ako môže škodlivý softvér počítač napadnúť je niekoľko a závisí hlavne od typu škodlivého softvéru.

Pri vírusoch obsiahnutých v programoch (aplikáciách) začne vírus vyvíjať nejakú nepríjemnú alebo škodlivú činnosť a nákaza sa začne rozširovať hneď v okamihu, keď spustíme infikovaný program. Zdrojom takýchto vírusov býva podozrivý pirátsky kopírovaný softvér alebo počítačové hry získané nelegálnou cestou. Každý infikovaný program (súbor) sa stáva nositeľom vírusu a tým sa infekcia šíri.

Existujú neškodné vírusy, ktoré sa prejavujú len výpisom upozornení na obrazovku. Iné skupiny vírusov spôsobujú spomalenie alebo zrušenie systému. Najnebezpečnejšie skupiny vírusov odosielajú informácie z počítača či ničia samotné súbory. Existujú vírusy, ktoré ničia celé sektory pevného disku. Niektoré vírusy sa pokúšajú zničiť aj hardvér počítača.

Po rozšírení internetu, a predovšetkým jednej z jeho služieb – elektronickej pošty, sa začali objavovať nebezpečné vírusy šírené zasielaním a prijímaním správ. Mnoho vírusov, tzv. makrovírusov, sa do počítača môže dostať výmenou dokumentov –

napríklad stačí otvoriť infikovaný dokument vytvorený v programe Microsoft Word a vírus sa môže šíriť. Dobrým prostredím pre šírenie vírusov sú počítačové siete a zdieľané priečinky.

Existujú aj programy, ktoré zisťujú a kradnú citlivé informácie z počítača, a navyše ich bez súhlasu majiteľa počítača odosielať cudzej osobe. Sú to tzv. špionážne softvéry alebo spywery. Informácie, ktoré sú takto odcudzené môžu byť rôzne, od zoznamu mailových adries až po heslo do nejakého systému. Tieto informácie môžu byť útočníkom použité od nabúrania sa do mailovej schránky až po napadnutie systému (napr. bankového konta). Najnebezpečnejším typom spywaru je tzv. keylogger. Je to program, ktorý sleduje, zaznamenáva a odosiela stláčanie kláves cudzej osobe. Takto sa cudzia osoba môže dostať k našim heslám do emailu, k číslam kreditných kariet a pod.

V prípade, že je počítač nakazený, začne sa správať neštandardne. Medzi takéto javy môžu napríklad patriť:

- nevysvetliteľné zrútenia systému,
- pri štartovaní programu sa objavuje správa „Nedostatok pamäte ...“ resp. „Not enough memory“,
- v prípade, že je program spustený, objavujú sa neobvyklé chybové hlásenia,
- programy, ktoré predtým fungovali bez problémov, nie je možné spustiť.
- a pod.

6.2.3 Vedieť preveriť (skenovať) počítač s využitím antivírusového softvéru.

POSTUP PRI NAPADNUTÍ POČÍTAČA VÍRUSOM

Jedným prvkom ochrany počítača pred zavírením je **antivírusový program**. Mal by byť pokiaľ možno osvedčený, kvalitný a samozrejme aktuálny. Antivírusové programy vyhľadávajú, identifikujú nebezpečné súbory a ničia počítačové vírusy. Medzi najznámejšie antivírusy u nás patria NOD32 (od slovenskej firmy Eset), AVG, Norton Antivirus, McAfeeVirus Scan, Panda Antivirus...

Aj keď opatrnosti nikdy nie je dosť a ak aj dodržíme všetky rady a máme vždy spustený antivírusový program, môže sa objaviť na monitore správa, že sme boli napadnutý vírusom XY. Prvá a zásadná rada znie: **NESPANIKÁRIŤ**. Ak antivírusový program detekuje vírus alebo hrozbu pre náš počítač tak ho vie odchytiť a poradiť si s ním. Nakazenie počítača ľubovoľným vírusom je síce nepríjemná záležitosť, ale antivírusové programy s najnovšou aktualizáciou pre detekciu nových vírusov si s nimi spravidla vedia poradiť. Platí však aj to, že svojimi neuváženými krokmi môžeme situáciu len zhoršiť. Postup pri odstraňovaní vírusovej nákazy závisí od mnohých faktorov, napr. či sme pripojení do siete.

V prípade že zistíme prítomnosť vírusu v počítači, ktorý je napr. súčasťou celopodnikovej siete, je najlepšie:

- vypnúť počítač (sieťovým vypínačom),
- upovedomiť správcu počítačovej siete.

Vírus môže byť prítomný v operačnej pamäti počítača a rovnako aj na pevnom disku či inom záznamovom médiu. Vypnutím počítača môžeme zabrániť jeho ďalšiemu šíreniu v sieti. Dôležité je informovať o vzniknutej infekcii správcu počítačovej siete – vírus sa mohol rozšíriť aj na ďalšie počítače.

V prípade, že k infikovaniu počítača vírusom došlo na domácom počítači alebo na počítači, ktorý nie je pripojený do počítačovej siete, **postupujeme podľa inštrukcií antivírusového programu**. Najčastejšie máme k dispozícii dve cesty tzv. dezinfekcie (odstránenia vírusu zo súboru):

- **Liečenie súboru** je možné previesť vtedy, keď je antivírusový program schopný infekciu odstrániť zo súboru – súbor ostáva po „preliečení“ v poriadku a je ho možné používať ďalej pri práci.
- **Odstránenie infikovaného súboru** používame vtedy, keď antivírusový program síce napadnutý súbor identifikoval, ale nemôže vírus zo súboru odstrániť.

Ako teda otestovať počítač na prítomnosť škodlivého softvéru??

Antivírusové programy sú síce rôzne, ale princíp ich práce je podobný.


WINDOWS DEFENDER

Jednou z možností ako si chrániť počítač vo Windowse 10 je Windows Defender. Windows Defender Offline je výkonný nástroj na offline kontrolu počítača, ktorý sa spúšťa z dôveryhodného prostredia a bez toho, aby bolo potrebné spustiť operačný systém.

Po prvom spustení Windowsu 10 je Windows Defender zapnutý a aktívne pomáha chrániť náš počítač zisťovaním malvéru (škodlivého softvéru), vírusov a ohrození zabezpečenia. Windows Defender používa ochranu v reálnom čase pri kontrole všetkého, čo do svojho počítača sťahujete alebo v ňom spúšťate.

Windows Update sťahuje aktualizácie pre Windows Defender automaticky, aby sa udržiaval váš počítač zabezpečený a chránený pred hrozbami.

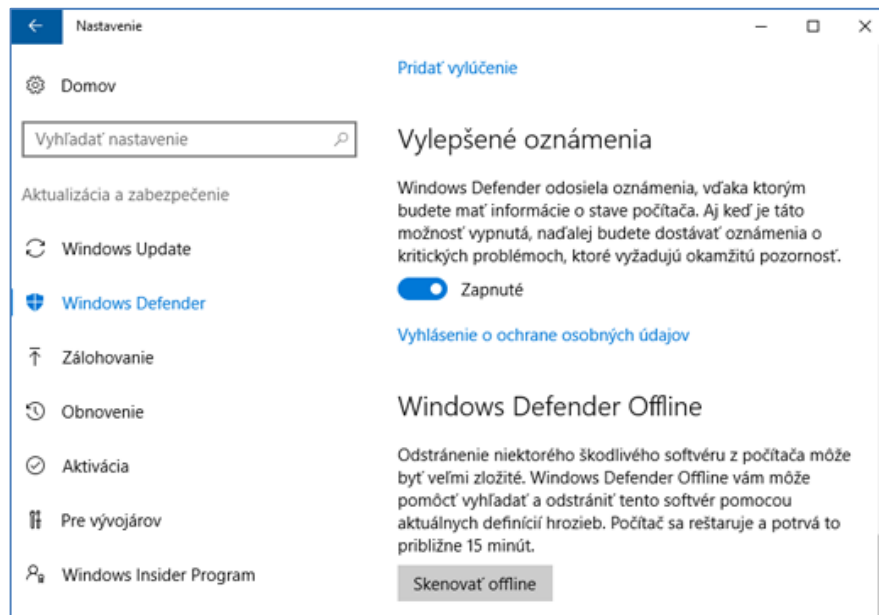
Zapnutie alebo vypnutie ochrany v reálnom čase vo Windows Defenderi

Vyberieme tlačidlo **Štart**  **→ Nastavenie → Aktualizácia a zabezpečenie**. Vyberieme položku Windows Defender a potom vypneme alebo zapneme ochranu v reálnom čase.

Windows Defender Offline

Ak sa domnievame, že v počítači máme skrytý malvér, ale softvér zabezpečenia nič nezistil môžeme spustiť kontrolu Windows Defendera Offline z nastavení Windows Defendera. Prejdeme na **Nastavenie → Aktualizácia a zabezpečenie → Windows Defender → Vybrať kontrolu offline**.

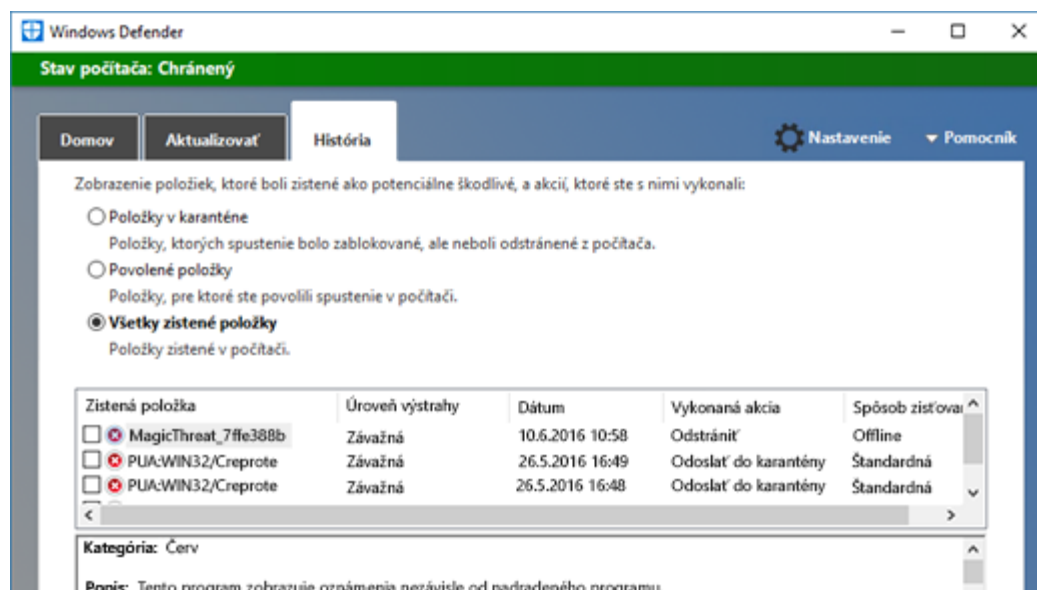
Kontrola Windows Defendera Offline trvá približne 15 minút a potom sa počítač reštartuje.



Ak chceme zobrazit' výsledky kontroly Windows Defenderom Offline:

Vyberte tlačidlo **Štart** a potom vyberte položky **Nastavenia** → **Aktualizácia a zabezpečenie** → **Windows Defender**.

Na karte **História** vyberieme položku **Všetky zistené položky** a potom položku **Zobraziť podrobnosti**. Všetky zistené položky Windows Defenderom Offline sa zobrazia ako offline v zdroji detekcie.



Ďalšou možnosťou je používať iný antivírusový program. My si opíšeme prácu s antivírusovým programom **ESET Endpoint Antivirus** od slovenskej firmy Eset spol. s.r.o. (www.eset.sk).

Štandardné nastavenia antivírusového programu ESET Endpoint Antivirus sú vhodné pre väčšinu užívateľov, preto odporúčame pri inštalácii akceptovať prednastavené hodnoty.

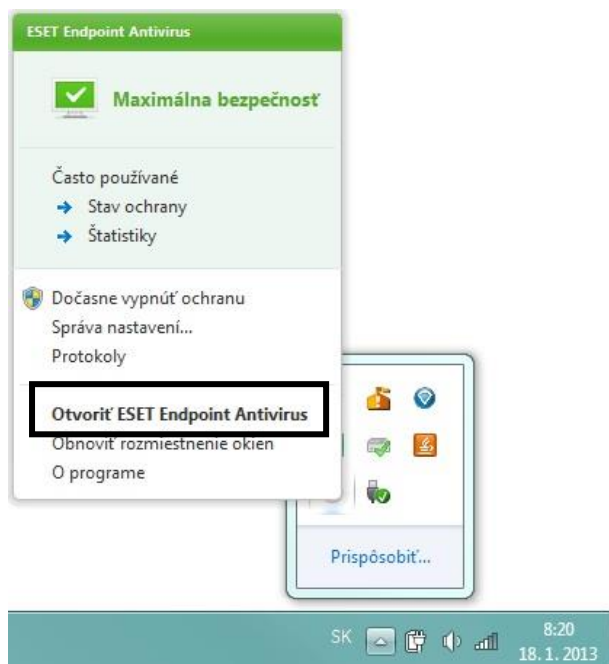
Pokročilým užívateľom umožňuje program prispôbiť si tieto nastavenia podľa svojich potrieb.

Na konci inštalácie budú všetky funkcie optimalizované pre konfiguráciu nášho počítača.

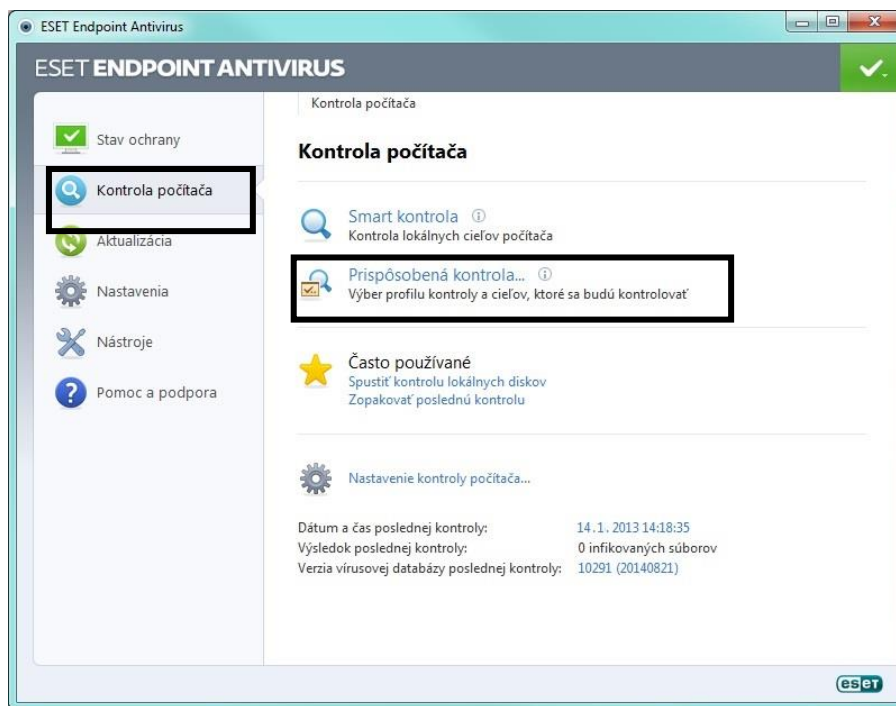
Existujú aj sieťové inštalácie, ktoré obsahujú niektoré ďalšie funkcie pre sieťové aplikácie.

Štandardne sa pri inštalácii antivírusového programu medzi ikonky v **Oblasti oznámení** na panely úloh zobrazí ikonka patriaca antivírusovému programu.

Po kliknutí na ikonu antivírusového programu sa nám zobrazí ponuka, z ktorej si vyberieme položku **Otvoriť ESET Endpoint Antivirus**.

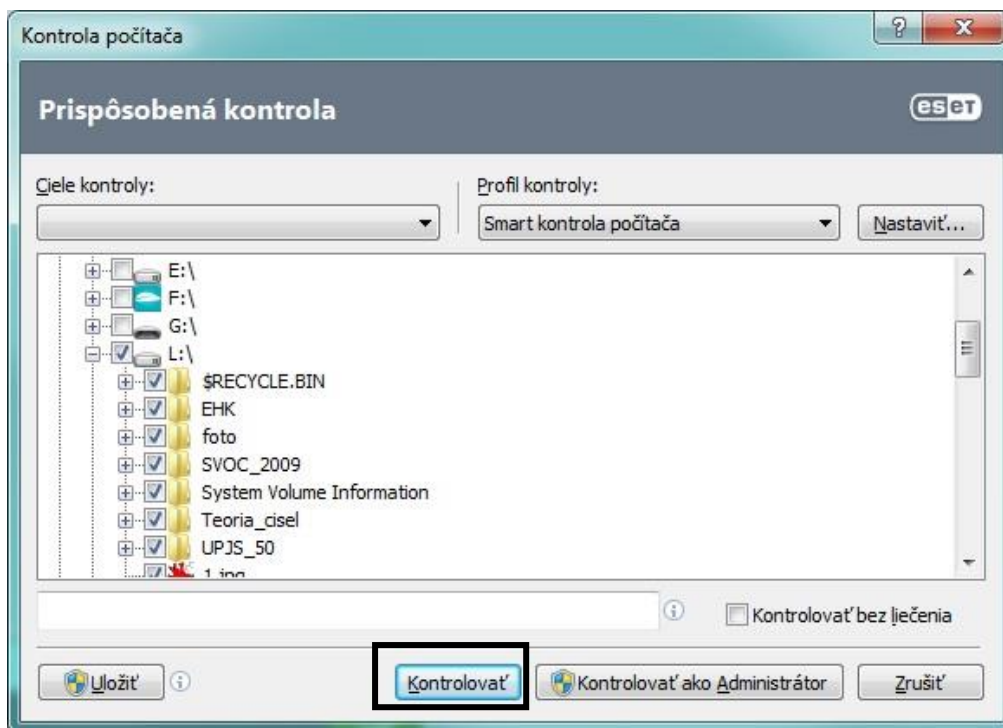


Otvorí sa okno antivírusového programu.



V Záložke **Kontrola počítača** klikneme na položku **Prispôsobené kontrola**.

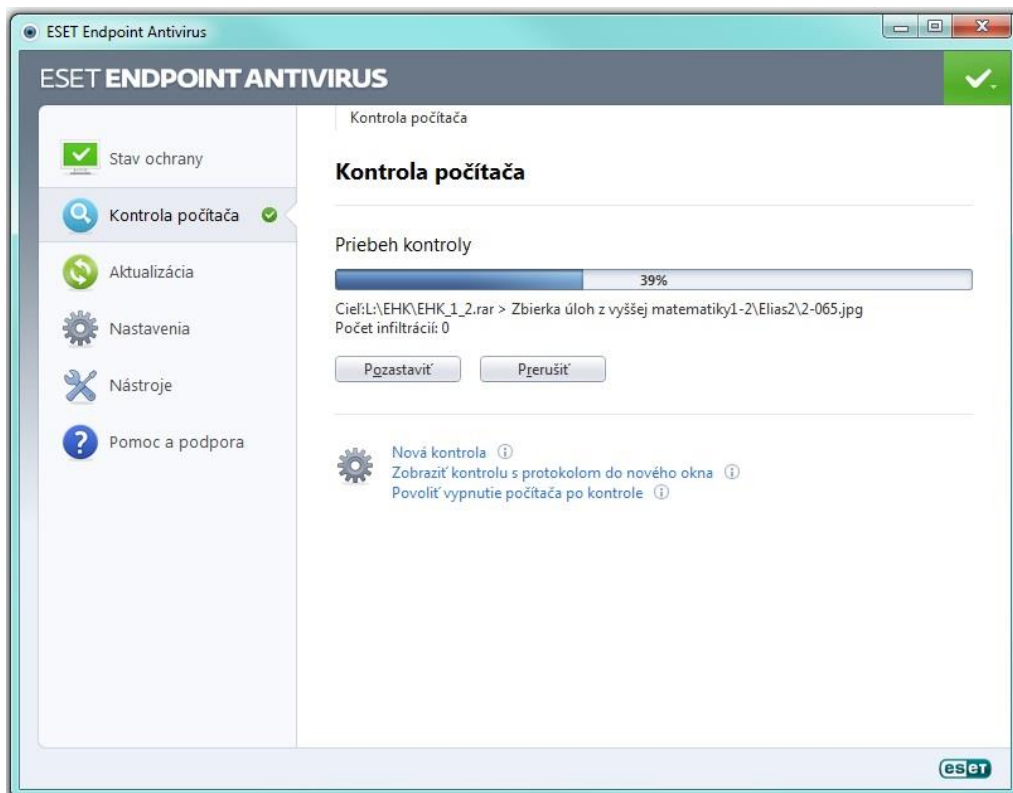
Otvorí sa okno v rámci ktorého si môžeme vybrať **profil kontroly** ako aj **ciele**, ktoré sa budú **kontrolovať**.



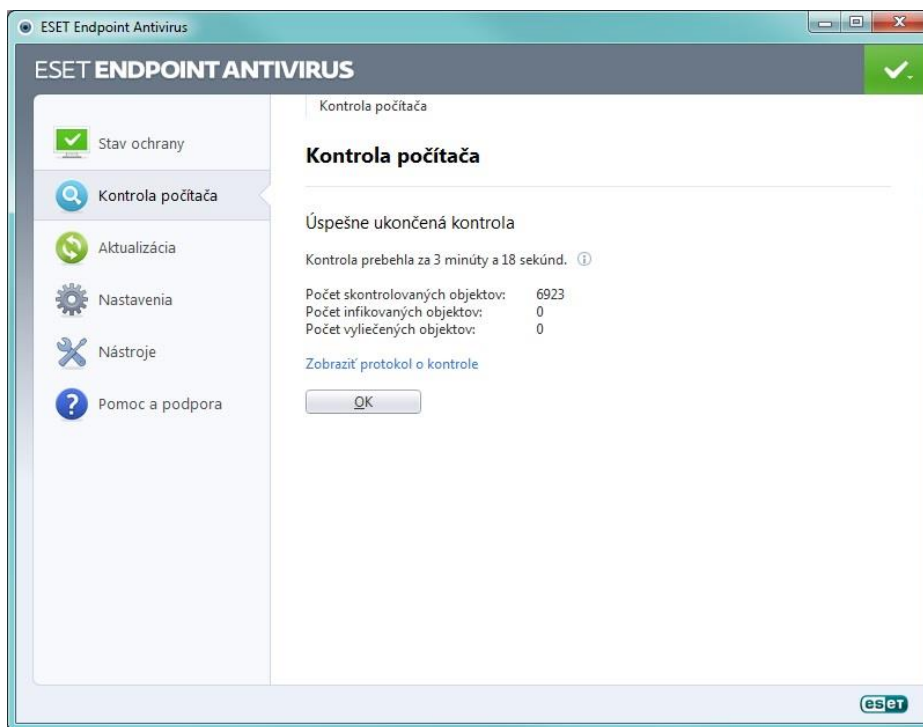
Zaškrtnutím políčka pri požadovanej položke (súbor, priečinok, diskovú jednotku) v ľavej časti okna si vyberieme tie položky, ktoré chceme otestovať. Položky rozbaľujeme klikaním na tlačidlo **+**.

Následne kliknutím na tlačidlo **Kontrolovať** spustíme antivírusovú kontrolu nami vybraných položiek.

Priebeh kontroly môžeme sledovať v okne.



Po ukončení diagnostikovania sa v okne aplikácie objaví **protokol o priebehu kontroly**. Nájde tu informáciu o tom, ktoré položky boli testované, počet diagnostikovaných položiek, počet nájdených vírusov a čas ukončenia.



6.3 Ochrana zdravia a životného prostredia pri IT

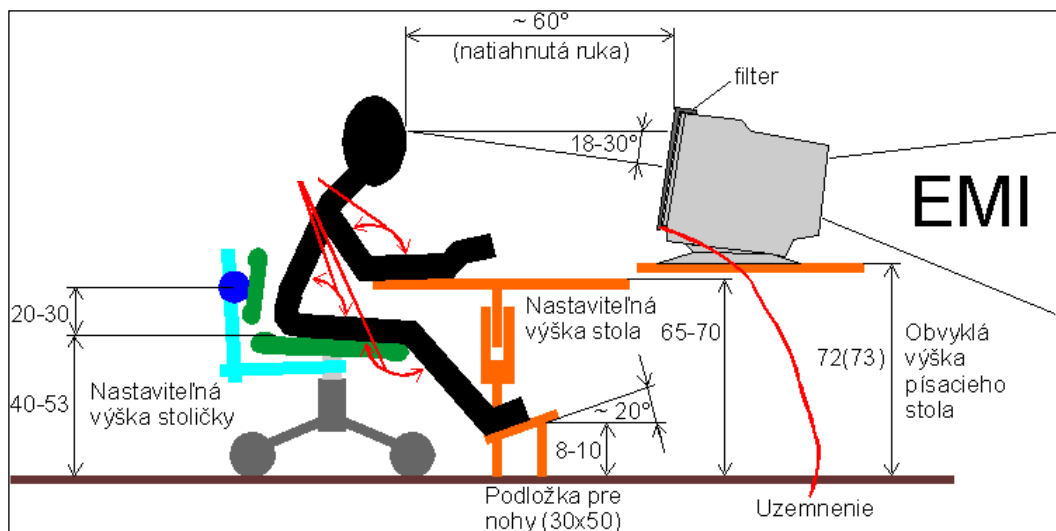
6.3.1 Chápať možnosti zlepšenia komfortu a pracovných podmienok pri práci s počítačom alebo zariadením, ako sú: pravidelné prestávky, zodpovedajúce osvetlenie, držanie tela.

ERGONÓMIA - PRVKY A NÁVYKY VYTVÁRAJÚCE DOBRÉ PRACOVNÉ PROSTREDIE

Na dobrú pracovnú atmosféru má vplyv množstvo faktorov. Dlhé hodiny pri počítači pôsobia skôr utlmujúco a demotivujúco, preto je vhodné striedať jednotlivé činnosti a prerušovať prácu hygienickými prestávkami.

Vo vetranej miestnosti s dostatkom kyslíka sa pracuje určite lepšie ako v kancelárii, do ktorej sa čerstvý vzduch dostane len sporadicky.

Pri práci s počítačom očakávame zvýšenie efektivity práce, ktorá súvisí s materiálnym zabezpečením. Náročnú prácu nemožno absolvovať pomocou nespoľahlivých, pomalých, na hranici svojich možností pracujúcich strojov. Dlhé čakacie doby na odozvu deprimujú pracovníka a vedú k strate motivácie. Tlač výsledkov na tlačiareň je potrebné tiež organizovať tak, aby hluk tlačiarne nerušil ostatných v práci. V prípade využívania spoločnej tlačiarne v sieťovej zostave nie je vhodné umiestniť ju do inej (napr. susednej) miestnosti. Hlučnosť sa síce takto dá odstrániť, ale v prípade nesprávneho príkazu sa zvyšuje nebezpečenstvo neželaného viacnásobného vytlačenia výsledkov alebo vzniku nepodarkov. Strata kontroly nad tlačiarňou neumožňuje včasné zakročenie na korekciu alebo zastaveniu takýchto dejov.



Odporúčané rozmiestnenie jednotlivých častí počítača a jeho príslušenstva je popísané na obrázku.

- **MONITOR** - v zásade platí, že **monitor** má byť položený na pracovný stôl tak, aby bol mierne **pod zorným uhlom pracovníka**, teda nie je vhodné ukladať

monitor na stôl na ležato položené počítače alebo inú polohu zvyšujúce predmety.

Monitor, rovnako ako TV prijímač, nikdy neumiestníme tak, aby bol za ním silný zdroj svetla alebo okno. Spôsobuje to tzv. fotografické videnie. Oči sa prispôbujú na vnímanie silne osvetlených častí a len s veľkou námahou môžu vnímať detaily na slabo svietiacej obrazovke.

- **KLÁVESNICA** - **klávesnicu** umiestňujeme tak, aby mal pracovník **dostatok miesta** na **prácu**, pričom **predlaktia** by **sa** mali **opierať o stôl**.
- **SKRINKA POČÍTAČA** - samotnú **skrinku počítača** neodporúčame ukladať priamo na podlahu. V prípade nízkeho umiestnenia pod stolom alebo vedľa stola je potrebné položiť ju na **mierne vyvýšený podklad**.

Poloha skrinky počítača má byť taká, aby neprekážala v pohybe a chladiaci ventilátor nenasával v blízkosti podlahy neustále víriaci sa prach, pričom obsluhu by mali byť disketové jednotky bez väčšej námahy dostupné.

VZÁJOMNÉ ROZMIESTNENIE POČÍTAČOV

Vzájomné rozmiestnenie počítačov býva veľmi často nesprávne. Viaceradové rozmiestnenie totiž nepovažujeme za vhodné. V predných radoch sediaci pracovníci sú neustále v pomerne veľkom magnetickom poli od zadnej magneticky málo tienenej časti monitora a rovnako sú aj ožarovaní alfa a gama žiarením. V takomto usporiadaní sú problémy aj s prírodnými a prepojovacími káblami.

Napríklad z hľadiska výučby a bezpečnosti je lepšie, ak sú počítače umiestnené v tvare "U". Monitormi vyžarované magnetické pole a častice sú vtedy tienené okolitou stenou budovy a na všetky pracoviská má učiteľ priamy pohľad. Jeho kontrolná a riadiaca činnosť nie je nijak obmedzovaná. Nie sú problémy ani s káblami, ani s úbytkovým zadným vyžarovaním monitorov.

STOLIČKY

Veľmi dobrými pre zabezpečenie zdravej a bezpečnej práce sa ukazujú stoličky, ktorých výška je variabilná (nastaviteľná). Výhodné sú stoličky s nastaviteľným operadlom.

OSVETLENIE, FAREBNÁ A AKUSTICKÁ ÚPRAVA

Osvetlenie, farebná a akustická úprava kancelárskych i laboratórnych priestorov býva len málokedy uspokojivo riešená. Snáď preto, lebo ich vplyv na prácu a výkonnosť pracovníkov nie je zistiteľná jednoduchými prostriedkami a tak veľmi často je ich vplyv podceňovaný. Osvetlenie v priemysle a v kanceláriách rieši norma STN 36 0451.

Osvetlenie denným svetlom možno ovplyvniť hlavne voľbou správnej orientácie a polohy laboratórnych miestností.

6.3.2 Rozumieť zásadám šetrenia energiou pri práci s počítačmi a zariadeniami ako sú: vypínanie, nastavenie automatického vypnutia, osvetlenie zozadu, nastavenie režimu spánku.

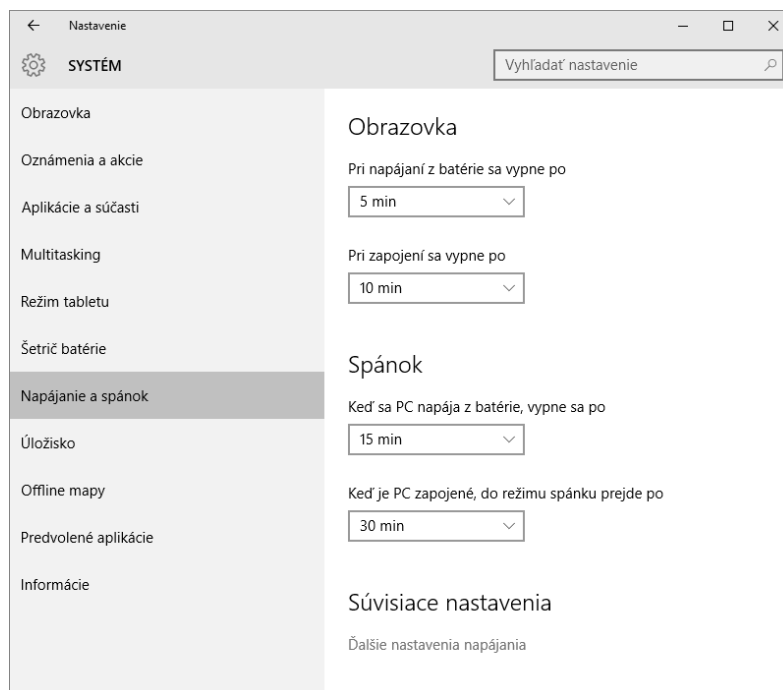
ZNIŽOVANIE SPOTREBY ENERGIE – VPLYV NA ŽIVOTNÉ PROSTREDIE

Peňazí nikto nemá nikdy nazvyš. Preto, ak si nechceme odopierať veci, ktoré máme nesmierne radi, naučme sa šetriť na veciach, ktoré nás zbytočne okrádajú.

Možno ste si ani neuvedomili, ale aj pri práci s počítačom môžeme ušetriť nemalé množstvo energie, teda peňazí.

Aké zásady šetrenia energiou by sme mali pri práci s počítačom dodržiavať?

- **Vypínajte počítač** – je nutné si uvedomiť, že aj keď na počítači nepracujeme, stále pohlcuje až 70% energie.
- Namiesto CRT monitora, **LCD monitor** – nielenže šetrí miesto a ponúka stabilný obraz, ale LCD monitor podstatne šetrí aj energie.
- **Na prehrávanie** hudby alebo filmov používajte **CD resp. DVD prehrávače**. Pri používaní počítača je totiž spotreba energie podstatne vyššia.
- Využívajte **efektívne nastavený režim spánku a automatického vypnutia**. Pre nastavenie režimu spánku alebo automatického vypnutia prejdite do menu **Štart** → **Nastavenie** → **System** → **Napájanie a spánok** → **Zmeniť čas prechodu počítača do režimu spánku**.



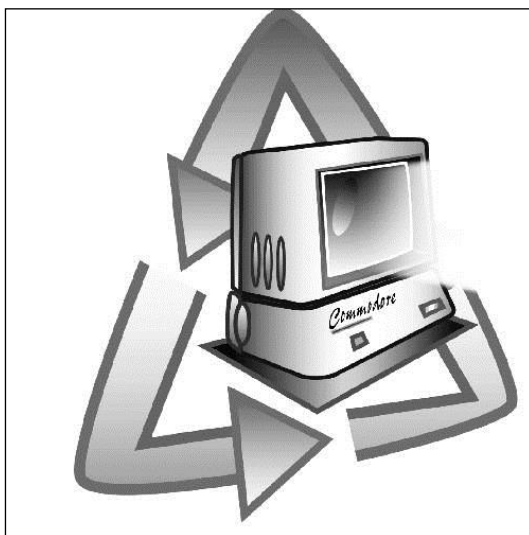
- **Vypínajte všetky zariadenia**, ktoré sú k počítaču pripojené a práve ich nevyužívate napr.- tlačiareň, reproduktory, a pod., pričom sa to týka aj Wi-Fi, infračerveného portu a Bluetooth.
- **Miestnosť vetrajte a počítač chlad'te**. Prehrievanie každého spotrebiča zvyšuje spotrebu elektrickej energie. To isté platí aj pri počítači. Preto je

vhodné zabezpečiť dostatočné vetranie nielen miestnosti, v ktorej sa počítač nachádza, ale podporiť aj samotné chladenie počítača (napr. chladiaca podložka pri notebookoch a pod.)

6.3.3 Chápať potrebu recyklácie počítačov, zariadení, batérií, tonerov, papiera.

ZNÍŽOVANIE SPOTREBY ENERGIE – VPLYV NA ŽIVOTNÉ PROSTREDIE

V čase rizika energetickej krízy a poškodzovania životného prostredia si musí asi každý z nás uvedomiť, že recyklovanie tlačných výstupov, recyklovanie tlačových kaziet s tonerom, používanie monitora, ktorý umožňuje znižovať spotrebu energie, šetrí životné prostredie, umožňuje prispieť k stabilizácii a zlepšeniu životného prostredia. So samotnou recykláciou sa na Slovensku



začalo pomerne neskoro. Mnohé obchodné spoločnosti a banky, aby nemuseli platiť peniaze za likvidáciu starého a opotrebovaného hardvéru, radšej darujú takéto počítače školám, z ktorých sa stávajú zbory starého „železa“. Spoločnosť si musí uvedomiť, že dodržiavaním pravidiel, recykláciou a šetrením elektrickej energie prispieva k zlepšeniu podmienok života na Zemi.

ZNÍŽOVANIE POTREBY TLAČENÝCH MATERIÁLOV NA ÚKOR ELEKTRONICKÝCH

S touto časťou je možné polemizovať, nakoľko k očakávanému zníženiu spotreby papiera po zavedení elektronickej korešpondencie a vytváraním elektronických materiálov nedošlo. Naopak, v celosvetovom priemere sa spotreba papiera v kanceláriách zvýšila. Väčšina ľudí uprednostňuje text vytlačený na papieri, ako jeho čítanie z obrazovky počítača, ktoré je oveľa náročnejšie. S rozvojom a miniaturizovaním niektorých zariadení sa možno dočkáme obratu aj v tomto smere a elektronické materiály nahradia tlačené. Problém je aj s archiváciou papierových dokumentov. Skriňu plnú papierových dokumentov už v niektorých podnikoch a firmách nahradili malými trezormi, v ktorých sa nachádzajú kompaktné disky s naskenovanými dokumentmi. Samotná záloha a povinnosť uchovávať napr. výsledky testov niekoľko rokov nútia organizácie pristupovať čoraz častejšie k elektronickému archivovaniu dôležitých dokumentov.

6.3.4 Poznať niektoré možnosti zvýšenia dostupnosti práce s počítačom, ako sú: softvér na rozpoznávanie hlasu, softvér na čítanie obrazovky,

obrazková lupa (screen magnifier), klávesnica na obrazovke (on-screen keyboard), vyšší kontrast.

V systéme Windows sú dostupné viaceré nastavenia, ktoré umožňujú zvýšiť dostupnosť práce s počítačom pre ľudí so zrakovým sluchovým resp. s pohybovým postihnutím. Medzi tieto nastavenia radíme softvér na rozpoznávanie hlasu, softvér na čítanie obrazovky, obrazková lupa (screen magnifier), klávesnica na obrazovke (on-screen keyboard) resp. vyšší kontrast

Tieto nastavenia môžete zapnúť a upraviť v časti **Zjednodušenie prístupu** v **Nastaveniach**.


PROGRAM NA ROZPOZNÁVANIE HLASU

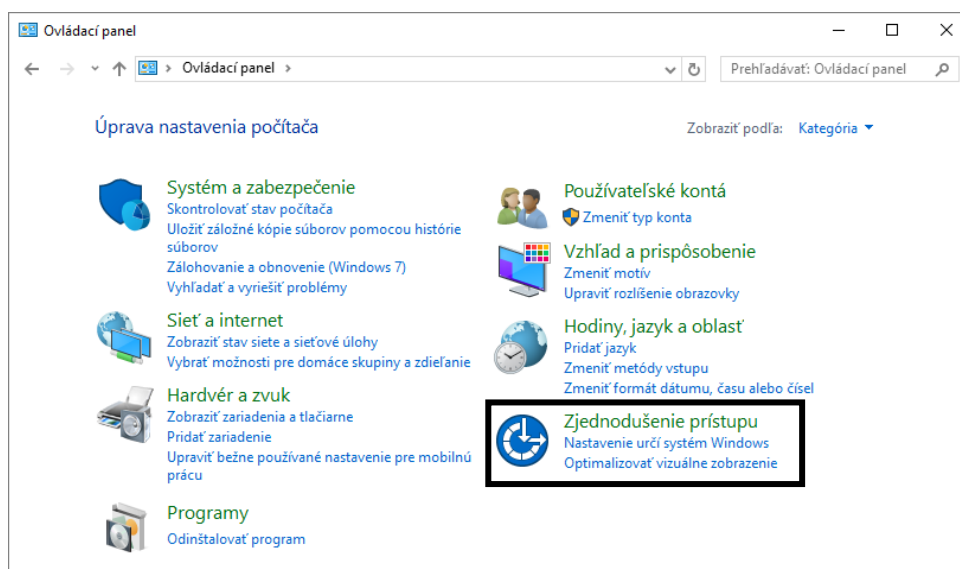
Program na rozpoznávanie hlasu umožňuje ovládať počítač hlasom. Pomocou mikrofónu môžete vyslovovať povely a príkazy, ktoré počítač rozpozná a bude na ne reagovať, alebo mu dokonca môžete diktovať text.

Úspech rozpoznávania reči úzko súvisí s kvalitou mikrofónu, ktorý používame. Poznáme dva najbežnejšie typy mikrofónov pre rozpoznávanie reči sú mikrofóny spojené so slúchadlami a mikrofóny stolové. Pri ovládaní počítača pomocou softvéru na rozpoznávanie reči je vhodnejšie používať súpravu slúchadiel a mikrofónu, pretože je menej náchylná na zachytávanie okolitých zvukov.

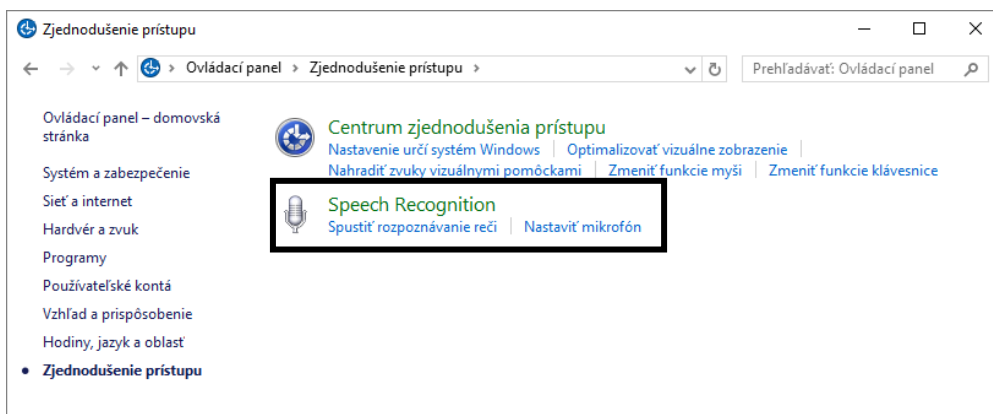
Je nutné podotknúť, že rozpoznávanie reči je k dispozícii iba v angličtine, francúzštine, španielčine, nemčine, japončine, zjednodušenej čínštine a v tradičnej čínštine.

Pre spustenie programu na rozpoznávanie hlasu je nutné dodržať nasledujúci postup:

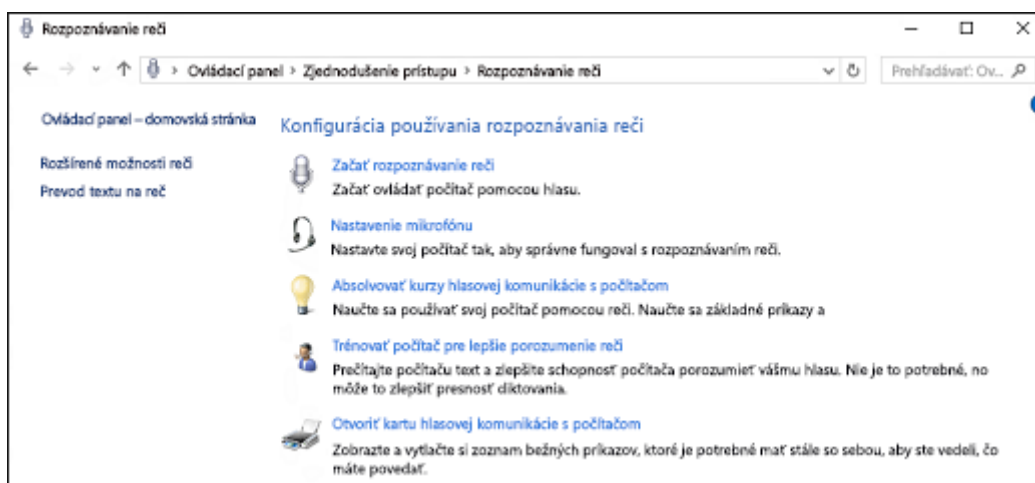
1. prejdeme do ponuky **Štart** , kde si zvolíme cez pravé tlačidlo myši možnosť **Ovládací panel**.



2. V rámci jednotlivých kategórií **Ovládacieho panela** si zvolíme kategóriu **Zjednodušenie prístupu**.



3. Pre otvorenie okna pre nastavenie a spustenie programu na rozpoznávanie hlasu sa vyberieme možnosť **Speech Recognition**, kedy sa nám otvorí okno v rámci ktorého si vieme základné parametre pre rozpoznávanie reči nastaviť.



Pred spustením programu na rozpoznávanie reči sa musíme ubezpečiť, že mikrofón je pripojený k počítaču a že je správne nastavený. základné nastavenia mikrofónu sa nachádzajú v časti **Set up microphone**.

Ak program spúšťame v našom počítači po prvý krát, je vhodné si tiež prejsť tutoriál t.j. tréningový program reči, ktorý Vám môže pomôcť naučiť sa používať správne príkazy tak, aby im Váš počítač rozumel. Výukový program trvá asi 30 minút a postupujte podľa pokynov, ktoré Vám sú v programe postupne zadávané. Tutoriál nájdeme v časti **Take speech tutorial**.

4. Samotný program na rozpoznávanie hlasu spustíme kliknutím na **Start Speech Recognition**.

A ovládanie počítača pomocou hlasových pokynov môže začať.


Poznámka - Rozpoznávanie reči je k dispozícii len v týchto jazykoch: angličtina (Austrália, India, Kanada, Spojené kráľovstvo a Spojené štáty), čínština (zjednodušená a tradičná), francúzština, japončina, nemčina a španielčina.

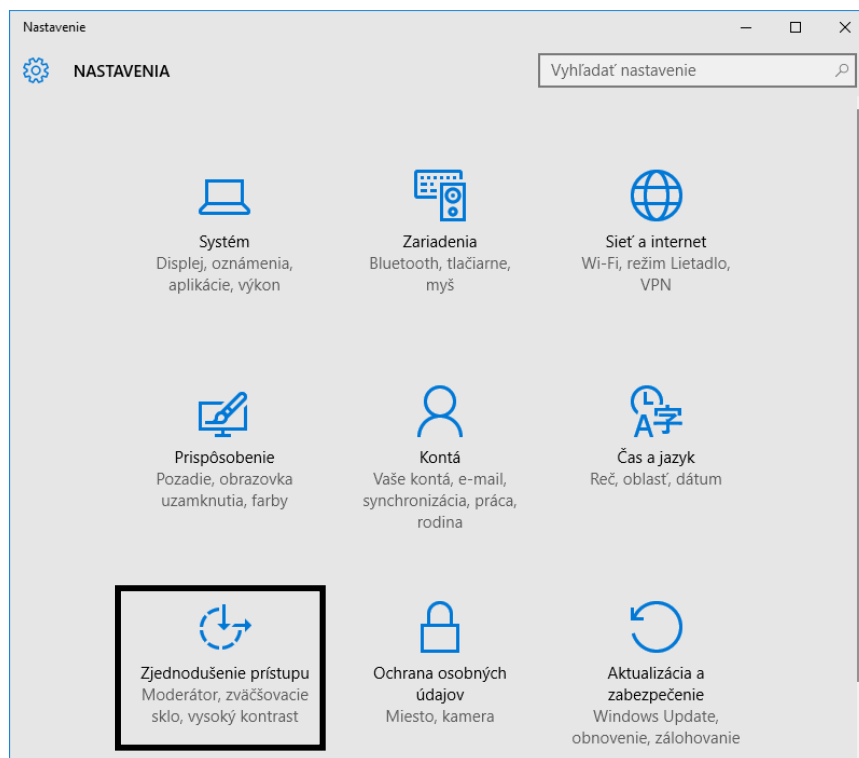
SOFTVÉR NA ČÍTANIE OBRAZOVKY – MODERÁTOR

Systém Windows obsahuje základný program na čítanie obrazovky – program **Moderátor**. Program Moderátor číta nahlas text zobrazený na obrazovke a popisuje niektoré udalosti (napríklad zobrazenie chybového hlásenia), ktoré sa vyskytujú pri práci s počítačom.

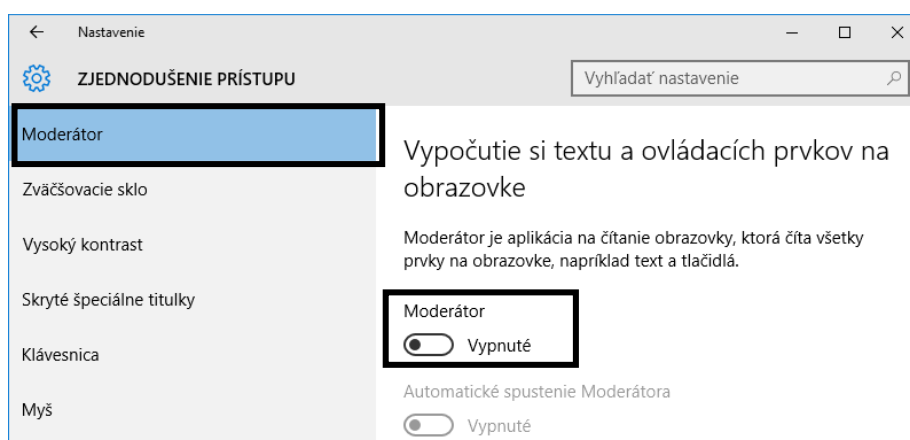
Je nutné podotknúť, že program Moderátor nie je k dispozícii vo všetkých jazykoch.

Pre spustenie **Moderátora** je nutné dodržať nasledujúci postup:

1. prejdeme do ponuky **Štart** , kde si zvolíme možnosť **Nastavenie**.

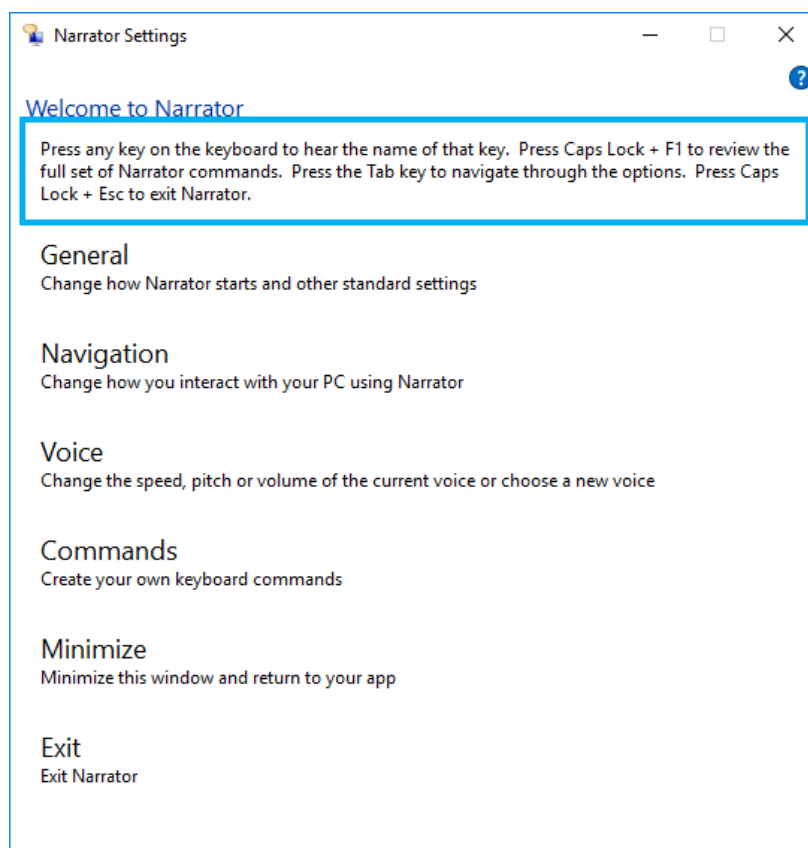




2. V rámci jednotlivých kategórií **Nastavení** si zvolíme kategóriu **Zjednodušenie prístupu**.



3. Otvorí sa nám okno **Zjednodušenie prístupu**, kde si vyberieme možnosť **Moderátor**. Moderátora zapneme prepnutím prepínača **Vypnuté** na **Zapnuté**.

4. Na pozadí sa otvorí sa okno Narrator Settings.



V aktualizácii Windows 10 Creators Update stlačte kombináciu klávesov **kláves s logom Windows**  + **Ctrl + Enter** a spustíte a zastavíte Moderátora. Opätovným stlačením týchto tlačidiel Moderátora zastavíte. V predchádzajúcich verziách Windowsu stlačte kombináciu klávesov **kláves s logom Windows**  + **Enter** a spustíte alebo zastavíte Moderátora. Mnohé klávesnice majú kláves s logom Windows umiestnený v dolnom riadku klávesov naľavo alebo napravo od klávesu Alt.

Ako určíme text, ktorý má moderátor čítať?

Na čítanie textu môžeme použiť aj režim skenovania. Ak chceme zapnúť režim skenovania, stlačíme **Caps Lock + medzerník**. Potom pomocou šípok nahor alebo nadol môžeme čítať riadok za riadkom a pomocou šípok doľava alebo doprava môžeme čítať po znakoch. Ďalšie informácie o režime skenovania sa nachádzajú v kapitole 3: Používame režim skenovania.

Ak chceme viac kontroly nad tým, čo čítame, Moderátor poskytuje príkazy na čítanie textu, ktoré pomáhajú v orientácii a čítaní textu na webových stránkach a v aplikáciách.

Ak chceme prečítať celý dokument alebo webovú stránku od začiatku, stlačíme kombináciu klávesov **Caps Lock + H**.

Ak chceme prečítať dokument od začiatku do miesta aktuálnej pozície kurzora, stlačíme kombináciu klávesov **Caps Lock + pravá hranatá zátvorka (])**.

Ak chceme čítať od aktuálnej pozície v dokumente alebo na webovej stránke, stlačíme kombináciu klávesov **Caps Lock + M**.

Ak chceme presunúť kurzor na začiatok dokumentu alebo webovej stránky, stlačíme kombináciu klávesov **Caps Lock + Y**.

Ak chceme presunúť kurzor na koniec dokumentu, stlačíme kombináciu klávesov **Caps Lock + B**.

Ak chcete prečítať aktuálnu stranu, stlačte kombináciu klávesov **Caps Lock + Ctrl + U**.


Ak chcete prečítať aktuálny odsek, stlačte kombináciu klávesov **Caps Lock + Ctrl + I**.

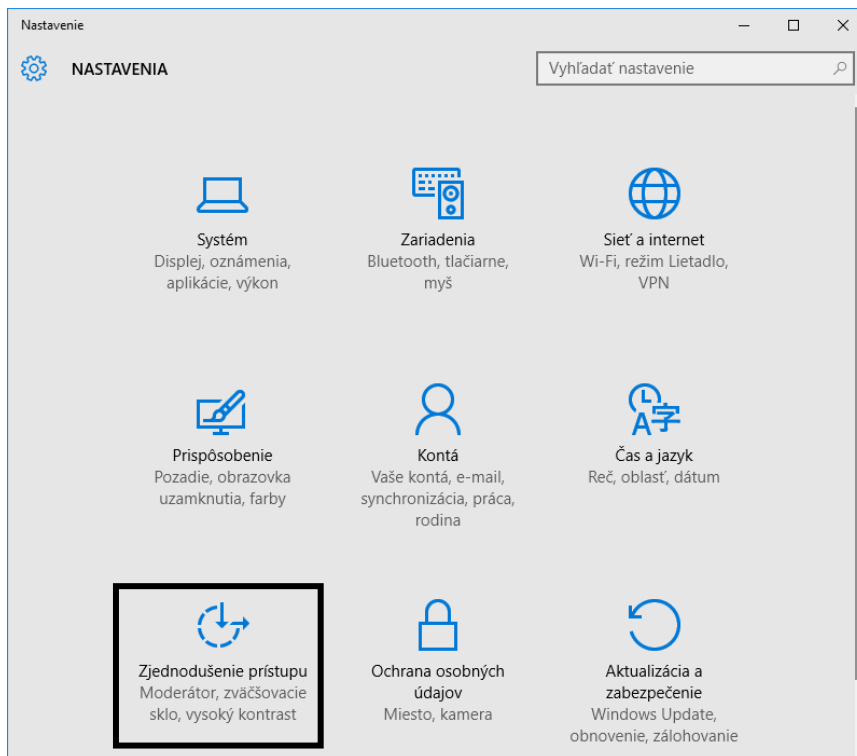
Ak chcete počuť atribúty formátovania, stlačte kombináciu klávesov **Caps Lock + F**.

OBRAZOVKOVÁ LUPA

Nástroj **Zväčšovacie sklo** zväčšuje rôzne časti obrazovky. Táto možnosť je užitočná na zväčšenie slabo viditeľných objektov, ale aj na jednoduchšie prezeranie celej obrazovky.

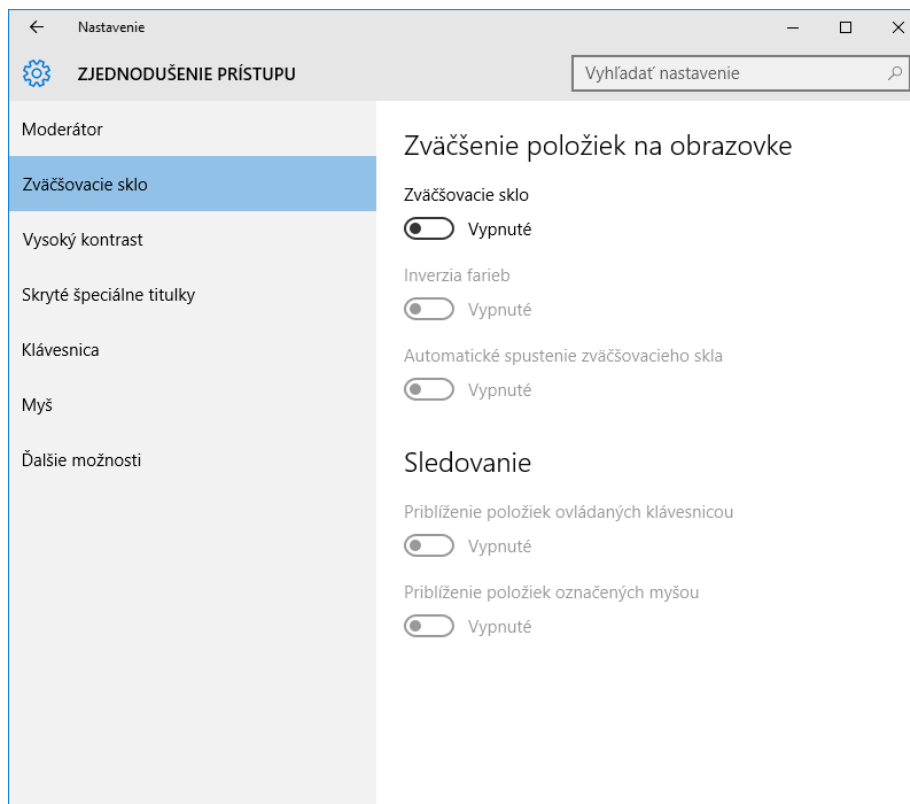
Pre spustenie **Obrazovkovej lupy – Zväčšovacieho skla** je nutné dodržať nasledujúci postup:

1. prejdeme do ponuky **Štart** , kde si zvolíme možnosť **Nastavenie**.

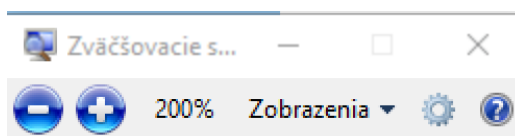



2. V rámci jednotlivých kategórií **Nastavení** si zvolíme kategóriu **Zjednodušenie prístupu**.


3. Otvorí sa nám okno **Zjednodušenie prístupu**, kde si vyberieme možnosť **Spustiť zväčšovacie sklo**.



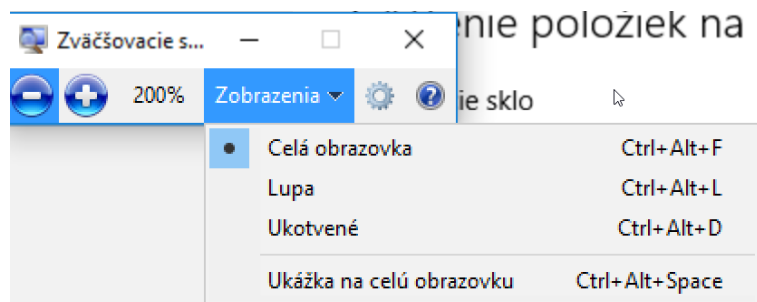
4. Automaticky sa spustí zväčšovacie sklo v zobrazení, ktoré sme mali naposledy použité a otvorí sa okno **Zväčšovacie sklo**.



V rámci daného okna máme k dispozícii tlačidlá  , ktorými vieme zväčšiť resp. zmenšiť percentuálne zväčšenie obrazovky.

Okno **Zväčšovacie sklo** sa nám po krátke doby zbalí do ikony  . Maximalizovať si ho opätovne vieme kliknutím na spomínanú ikonu.

Pri zväčšovaní skla máme tri režimy zobrazenia, ktoré si volíme po kliknutí na možnosť **Zobrazenia** v okne **Zväčšovacie sklo**.




- **Režim zobrazenia na celú obrazovku.** V režime zobrazenia na celú obrazovku sa zväčšuje celá obrazovka. Nástroj Zväčšovacie sklo potom môže sledovať ukazovateľ myši.
- **Režim lupy.** V režime lupy sa zväčšuje len oblasť okolo ukazovateľa myši. Pri posúvaní ukazovateľom myši sa zväčšovaná oblasť obrazovky pohybuje spolu s ukazovateľom.
- **Režim ukotvenia.** V režime ukotvenia sa zväčšuje iba časť obrazovky a zvyšok obrazovky zostáva v normálnom zobrazení. Používateľ vyberá oblasť, ktorá oblasť obrazovky sa zväčší.

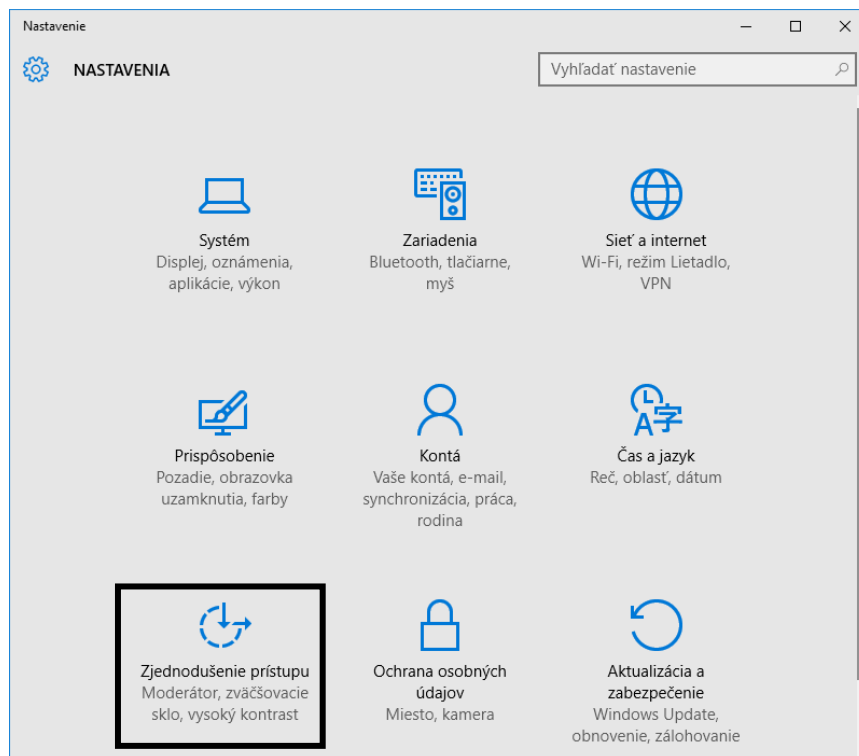
Zväčšovacie sklo zrušíme prepnutím na **Zväčšovacie sklo** na **Vypnuté** alebo stlačíme kláves s logom systému **Windows+Esc**.

KLÁVESNICA NA OBRAZOVKE.

Pri písaní a zadávaní údajov môžete namiesto fyzickej klávesnice použiť program **Klávesnica na obrazovke**. V programe **Klávesnica** na obrazovke sa zobrazí vizuálna klávesnica so všetkými štandardnými klávesmi. Klávesy môžete vyberať pomocou myši alebo iného ukazovacieho zariadenia, alebo môžete použiť klávesy na bežnej klávesnici.

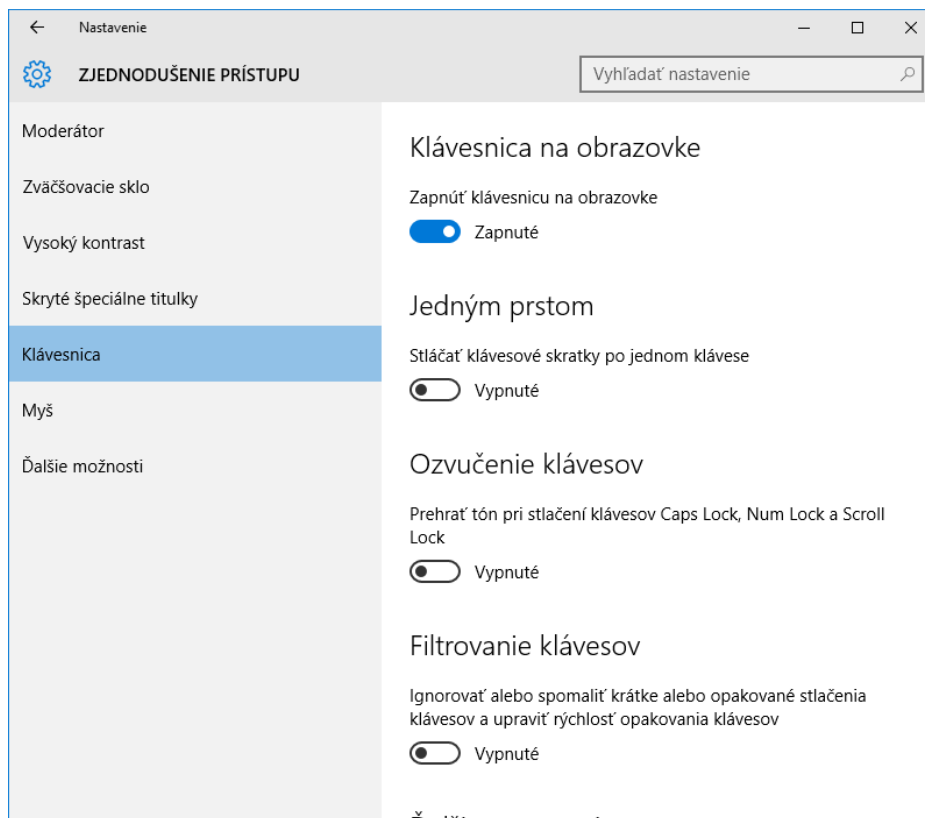
Pre spustenie **klávesnice na obrazovke** je nutné dodržať nasledujúci postup:

1. prejdeme do ponuky **Štart** , kde si zvolíme možnosť **Nastavenie**.

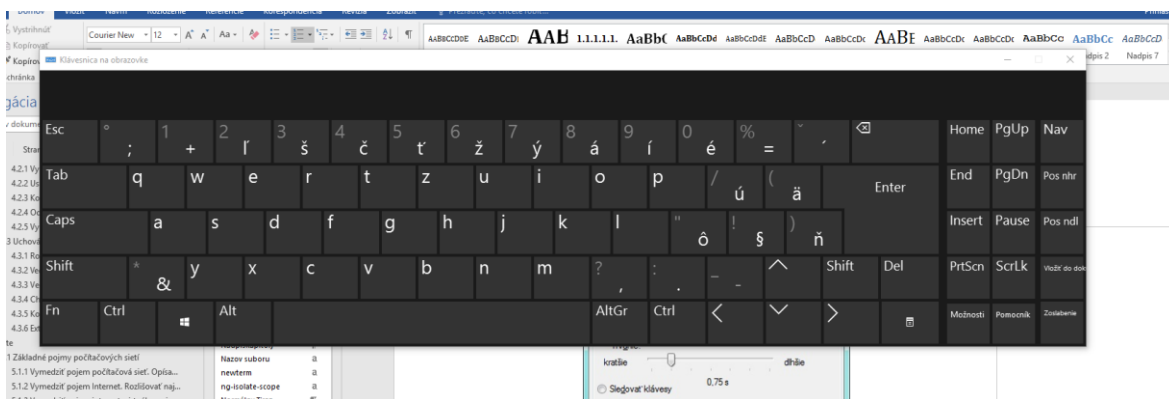


2. V rámci jednotlivých kategórií **Nastavení** si zvolíme kategóriu **Zjednodušenie prístupu**.

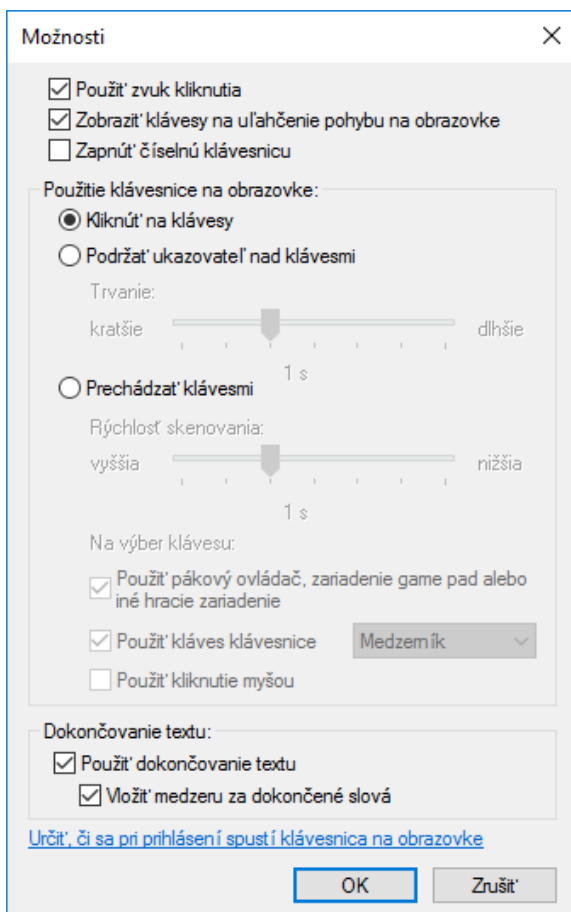
3. Otvorí sa nám okno **Zjednodušenie prístupu**, kde si vyberieme možnosť **Klávesnica**.



4. Automaticky sa nám spustí **klávesnica na obrazovke** a my môžeme zadávať text napr. do textového editora pomocou nej.



Nastavenia klávesnice môžeme zmeniť po kliknutí na tlačidlo **Možnosti**, kedy sa nám zobrazí dialógové okno základných nastavení klávesnice na obrazovke.

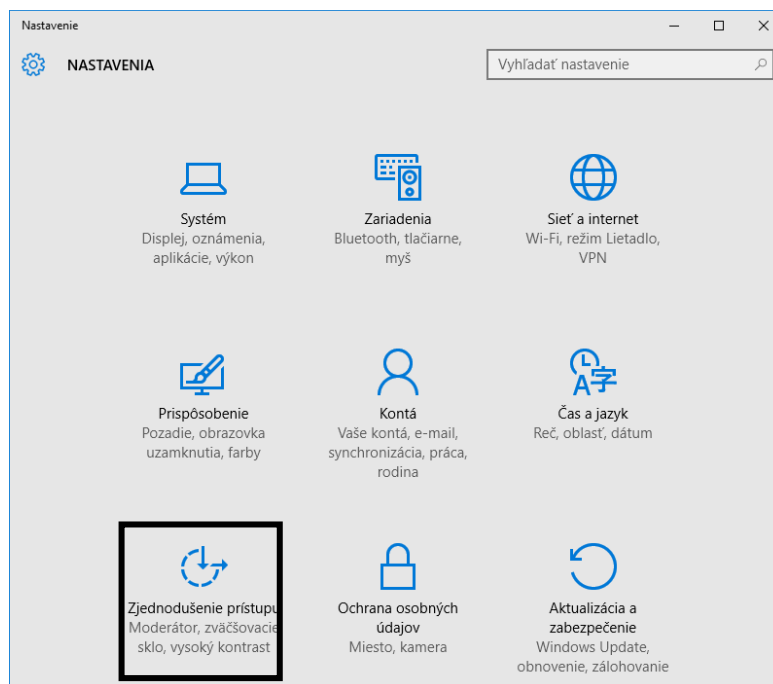


VYŠŠÍ KONTRAST

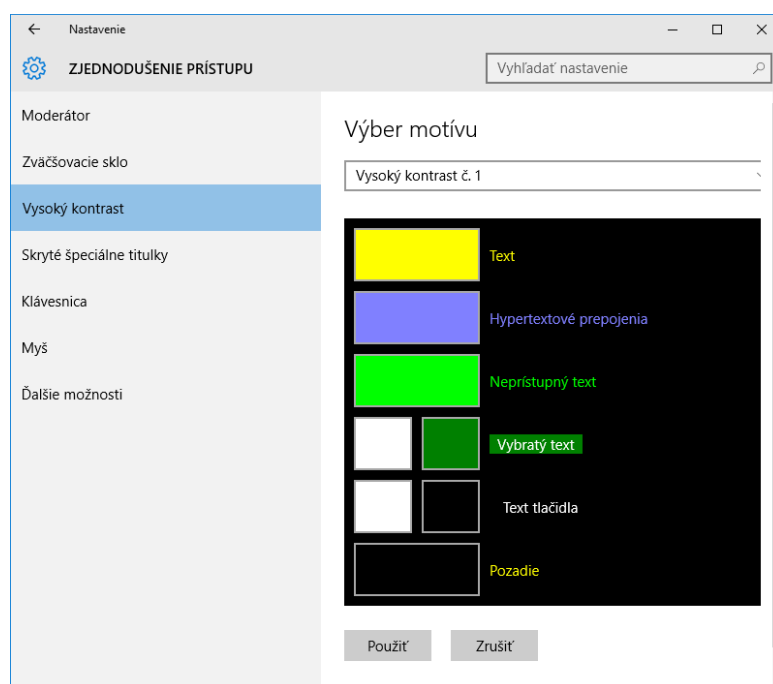
Poslednou možnosťou na zvýšenie dostupnosti práce s počítačom je možnosť nastavenia vyššieho kontrastu. Toto nastavenie nám umožňuje nastaviť farebnú schému s vysokým kontrastom, ktorá zvýši farebný kontrast niektorých textov a obrázkov na obrazovke počítača, čím sa zlepší ich viditeľnosť a zjednoduší identifikácia.

Pre spustenie klávesnice na obrazovke je nutné dodržať nasledujúci postup:

1. prejdeme do ponuky **Štart** , kde si zvolíme možnosť **Nastavenie**.



2. V rámci jednotlivých kategórií **Nastavení** si zvolíme kategóriu **Zjednodušenie prístupu**.
3. Otvorí sa nám okno **Zjednodušenie prístupu**, kde si vyberieme možnosť **Vysoký kontrast**.



4. Kliknutím na odkaz **Výber motívu** sa otvorí ponuka motívov s vysokým kontrastom.
5. Zvolíme si jeden z ponúkaných motívov s vysokým kontrastom a kliknutím ho potvrdíme.