

Vysoká škola ekonomická

Fakulta informatiky a statistiky

Katedra systémové analýzy

Měnící se význam a vliv informací

vypracoval: Jan Láznička

vedoucí práce: Ing. Antonín Rosický, CSc.

rok 2007

Prohlášení autora

Prohlašuji, že tuto bakalářskou práci, jejíž téma je „Měníci se význam a vliv informací“, jsem zpracoval sám. Veškerou literaturu a ostatní zdroje, z kterých jsem při psaní vycházel, jsem uvedl na závěr práce do Seznamu použitých zdrojů.

V Praze, 9. května 2007

Jan Láznička

Exekutivní shrnutí

Bakalářská práce, pro kterou jsem si vybral téma „Mění se význam a vliv informací“, se zabývá nejprve podstatou lidského myšlení, protože právě v mozku dochází k procesům, které nám dovolují informace chápat, ukládat si je do paměti, pracovat s nimi. Jsou zde nastíněny důvody, proč se jednání lidí různí, i pokud mají stejné údaje, a porovnány možnosti rozhodnutí založených právě na jedinečnosti každého člověka. Samozřejmostí při práci s informacemi jsou informační zdroje, v textu popsány s ohledem na minulou dobu a současnost. Se zdokonalujícím se prostředím informačních a komunikačních technologií a nárůstem počtu informací a jejich důležitosti, je kladen velký důraz na důsledné zabezpečení informací. Proto jsou zde rozepsány i základní šifrovací algoritmy, které se používají v kryptologii. Závěr práce je věnován náhledu na budoucnost práce s informacemi.

1	Úvod	7
2	<i>Jak člověk informace chápe a jak jim rozumí</i>	9
2.1	Co bychom měli vědět o lidském chápání informací	9
2.2	Informace a její různé definice	10
2.3	Mozek jako centrum lidského chápání	12
2.4	Význam jedinečnosti (osobnostního fondu) každého člověka	15
2.5	Vliv výchovy, sociálního a kulturního prostředí na individuálnost jedince	17
3	<i>Informace jako základ lidského jednání a rozhodování</i>	19
3.1	Člověk jedná v závislosti na informacích	19
3.2	Nutnost získávání informací	19
3.3	Na co si dát při hledání informací pozor	21
3.4	Rozdílnost řešení projektů na základě informovanosti	23
4	<i>Zdroje informací, odkud čerpáme dnes a odkud v minulosti</i>	26
4.1	Kde začínáme hledat informace	26
4.2	Prapočátky sdělování informací	27
4.3	Nosiče informací	27
4.4	Tištěné zdroje informací	29
4.5	Elektronické zdroje informací	31
4.6	Ostatní zdroje dat	33
5	<i>Ochrana proti zneužití informací</i>	34
5.1	Bezpečnost je důležitá	34
5.2	Co je to kryptologie	35
5.3	Historie Kryptologie	37
5.3.1	Starověk	37
5.3.2	Středověk	39
5.3.3	Dvacáté století	39
5.3.4	Současnost	40

5.4	Steganografie	40
5.5	Symetrická kryptografie	41
5.6	Asymetrická kryptografie	42
5.7	Hašovací funkce	44
6	<i>Náhled na možný budoucí stav přístupu k informacím</i>	46
6.1	Počítačová gramotnost	46
6.2	Představa vývoje přístupu k informacím	47
7	<i>Závěr</i>	49
8	<i>Seznam použitých zdrojů</i>	51
9	<i>Seznam obrázků</i>	53

1 Úvod

Téma „Měníci se význam a vliv informací“ jsem si vybral z toho důvodu, že stále více je potřeba v dnešním světě mít ty správné informace, aby byl člověk úspěšný. Ale ne každý je dokáže získat, a ne každý s nimi umí pracovat tak, jak by bylo optimální. Mým cílem tedy bude nastínit některé aspekty práce s informacemi s ohledem na jedinečnost každého člověka a vývoj technologických možností, které tuto práci usnadňují.

Následující práce se tedy bude týkat informací a jejich měnícího se významu a vlivu v lidské společnosti. Dostatek relevantních informací je stále důležitější a důležitější pro správné rozhodování a efektivní chování lidí. Oproti minulým desetiletím a staletím je význam informací v dnešní době poněkud jiný. Jednak jich máme k dispozici stále více, můžeme se učit i z chyb našich předků, a jednak je člověku práce s nimi stále zjednodušována a ulehčována pomocí nových informačních a komunikačních technologií.

Ovšem abychom dokázali naplno využívat informace, musíme vědět, co se děje při získávání informací v mozku, a znát důvody, proč jsou lidé v přemýšlení a uvažování tak rozdílní, i pokud obdrží stejné údaje. Jedinečnost lidí, jejich osobnostního fondu, je do značné míry ovlivněna výchovou a sociálním a kulturním prostředím, ve kterém vyrůstáme. Názorný příklad jiného řešení problému dříve a dnes, tedy v obdobích, kdy máme k dispozici naprosto jiné informace, si ukážeme konkrétně na stavbě nového letiště.

Abychom získali informace, po kterých toužíme, je nutné nejprve zvolit správný zdroj, ze kterého budeme informace čerpat. Jaké jsou vůbec možnosti při volbě takovýchto zdrojů? Stručně si je zmíníme, od prapočátků sdělování informací, přes knihovnické služby až po elektronické nosiče informací a internet, který má v sobě obrovský potenciál i do budoucna, nejen jako informační zdroj.

Jak již byla řeč, informace jsou stále důležitější, proto se stávají i více ohrožené a musíme si je více chránit. S narůstajícími možnostmi při využití počítačů a internetu se rozrůstá také počet útoků a pokusů o nelegální získání důvěrných

informací. Měli bychom se snažit tomu zabránit, jelikož s internetem pracuje stále více lidí a právě z internetu hrozí v poslední době nejvíce útoků. Tomuto problému se bude věnovat celá kapitola o bezpečnosti informací, více zaměřená na kryptologii.

Na závěr práce bude nastíněn možný budoucí stav přístupu k informacím, protože jejich význam a vliv se neustále mění, zesiluje. Také zde najdete krátké pojednání a uvažování o počítačové gramotnosti, která se stává nutností pro větší pravděpodobnost získání dobré pracovní pozice. I proto je důležité v budoucnu věnovat práci s informacemi velkou pozornost.

2 Jak člověk informace chápe a jak jim rozumí

2.1 *Co bychom měli vědět o lidském chápání informací*

Nejprve je nanejvýš vhodné zmínit se o pár faktech. Nastínit si, co to vlastně je informace, objasnit tento pojem, připomenout některé definice informací, s kterými se můžeme v různých publikacích setkat.

Stejně tak důležité je porozumět převelice důležitému a nesmírně složitému lidskému orgánu, mozku, neboť právě mozek je tím centrem všeho lidského vědění, poznání, všech informací, které k nám přicházejí, a které si uchováme a zapamatujeme, nebo je zapomeneme tak rychle, že si to ani neuvědomíme. Mozek je opravdu pozoruhodný a určitě si zaslouží, abychom věděli, jak pracuje, respektive jak vůbec jsme jako lidé schopni se učit, rozvíjet svou osobnost, poznávat nové věci, uchovat si je v paměti, osvojit si je.

Ovšem učení se a osvojování si určitých pravidel je do značné míry ovlivněno tím, jak člověk roste, dospívá, v jakém žije prostředí, jaké má návyky vrozené, nebo odkoukané. Není moc lidí, kteří by dokázali úplně zapomenout na určité více méně rutinní postupy, jen proto, že by chtěli žít úplně jiným, novým život. Je to vůbec možné? Je v lidských silách vědomě ztratit všechny návyky a učit se znovu a sám? Důležité je v předešlé otázce slovo „vědomě“, protože samozřejmě známe případy, kdy se stane nějaký úraz, nehoda, a lidé pak sami nevědí, jak například zapnout sporák. Ale těmito případy se zde zabývat nebudeme.

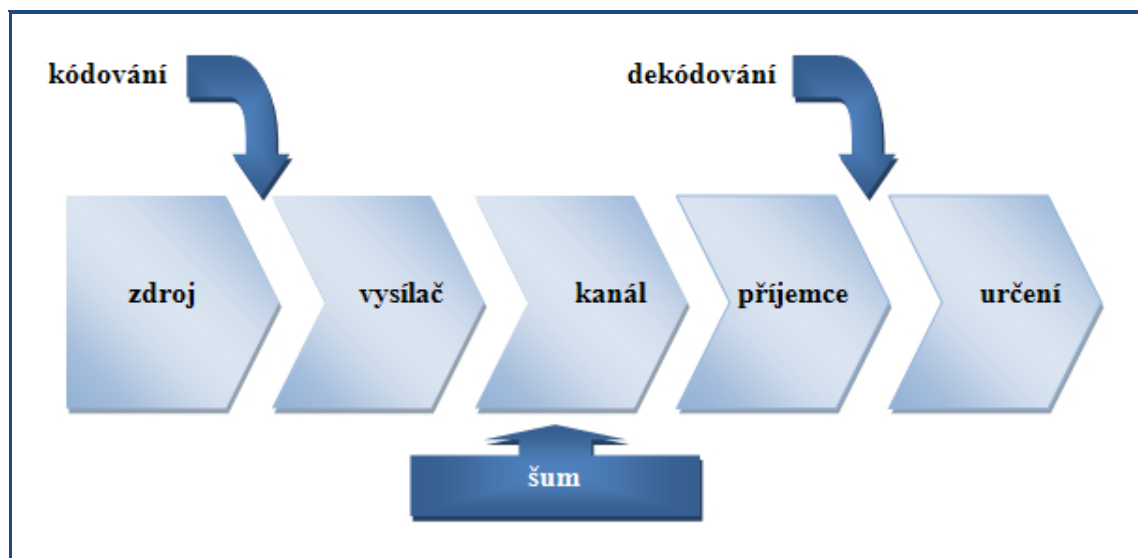
Každý z nás vyrůstal někde jinde, měl jiné rodiče, zázemí. A právě rodiče hrají nejdůležitější roli v dětství každého jedince, neboť mu ukazují, jak žít. Dalo by se říci, že pro nás představují návod, jak se chovat v určitých situacích. Ne nadarmo se říká, že jablko nepadá daleko od stromu. Vedle rodičů mohou existovat různé vzory, které se snažíme napodobit, přiblížit se jim jak stylem oblékání, mluvení, tak i způsobem chování. Prostě a jasně řečeno, záleží na kulturním a sociálním prostředí, ve kterém se pohybujeme.

2.2 Informace a její různé definice

Pojem informace je těžko definovatelný a můžeme se setkat s mnoha různými teoriemi a náhledy na to, co toto slovo znamená.

Jak uvádí Jiří Cejpek /4/, slovo informace pochází z latiny, konkrétně zde můžeme nalézt dva „kořeny“ původu tohoto pojmu. Jednak latinské „informare“ znamená uvádět ve tvar, dodávat tvar, podobu, formovat, tvořit, zobrazovat, představovat, vytvářet představu, pojem. Další latinské slovo „informatio“ vyjadřuje představu, pojem, obrys. Je zde tedy patrná souvislost s lidským vědomím, chápáním. A opravdu, s informacemi, respektive s tímto pojmem, se lidé setkávají dennodenně, a neustále hledají nové a nové informace, ať už se jedná o to, jaký film si vybereme pro večerní relaxaci v kině, nebo jakou metodu použít při výběru nejvhodnějšího projektu pro svou firmu. Je jasné, že pokud by tyto dva hypotetické problémy řešilo více lidí, každý by volil jinou cestu, jak dané informace získat. Podrobněji si to ukážeme v jedné z následujících kapitol.

Existují různá pojetí informace, například Norbert Wiener říká, že „informace je informace a není ani hmotou, ani energií“. Stejně tak poznamenává, že „informace je obsah toho, co si vyměňujeme s okolním světem, když se mu přizpůsobujeme a působíme na něj svým přizpůsobováním“. Tato definice koresponduje s tradiční Shannonovou teorií informace, která znázorňuje koncept informace jako komunikační teorii, jejíž schematické znázornění je uvedeno na obrázku 2.1. Shannonova teorie činí vlastně informaci nezávislou na médiu, informace je předávána od zdroje v zakódované podobě vysílačem přes komunikační kanál k příjemci, který ji dekóduje a poté vyhodnotí (zanalyzuje, uloží, atd.). K dekódování je nutná znalost kódovacího jazyka odesílatele informace, nebo postupu jak informaci dekódovat. V díle Svět moderního myšlení, /15/, je jazyk popisován jako univerzální prostředek k vyjadřování myšlenek (bez jazyka není myšlení, dokonce i přemýšlení se opírá o vnitřní řeč). Jednotlivé prožitky, odrazy skutečnosti zobecňujeme ve slovech, pojmech, kategoriích.



Obrázek 2.1 - Shannonova teorie informace - komunikační kanál

Ze Shannonovy teorie informace již vidíme patrnou souvislost s technickými normami, konkrétně ČSN 369001, která říká, že informace je význam, který člověk přisuzuje údajům (údaj, neboli datum, data, je dle ČSN obraz vlastností objektu, vhodně formalizovaný pro přesnost, interpretaci, nebo zpracování prostřednictvím lidí nebo automatů). Tato definice informace se mi zdá jako nejlépe vysvětlující, vyzdvihuje rozlišnost mezi informacemi a daty. Z této definice bychom mohli odvodit, že člověk přisuzuje datům určitý význam podle svých znalostí, každý člověk tedy určitým datům bude přisuzovat jiný význam. V následujícím textu bude toto téma ještě více rozvedeno.

Také internetová encyklopedie /20/ říká, že informace je výsledek vyhodnocování smyslových vjemů, zpracování nebo organizace dat. Přestože mnozí lidé hovoří o „informačním věku“, „informační společnosti“ a „informačních technologiích“, neexistuje jednotná definice tohoto termínu. Jeho význam se totiž může měnit podle kontextu a úzce souvisí s dalšími tématy, jako je znalost, návod, komunikace nebo poznání. Je zde informace chápána i ze stejného náhledu jako ji chápe Shannon, tedy že je to zpráva, kterou se vysílač rozhodl vytvořit a kde během putování k příjemci snižuje její srozumitelnost komunikační šum.

2.3 *Mozek jako centrum lidského chápání*

Mozek bychom mohli chápat jako jakýsi centrální bod lidského „informačního systému“, dokáže shromažďovat, zpracovávat, uchovávat a šířit informace. Vnější i vnitřní podněty, přicházející do mozku, jsou mozkem zpracovávány a výsledkem takového zpracování je pak poznatek. Ovšem nabízí se otázka, jak toto zpracování probíhá? Co je vlastně v mozku tak zázračného? Stručně si zkusíme popsat, jak takový mozek vypadá, jaké má části, z čeho vůbec mozek je.

Především si musíme uvědomit, že v mozku jsou dva typy buněk – neurony (je jich 10 až 15 miliard) a tzv. gliové (vyživovací) buňky, kterých je až desetkrát více než neuronů. Nervové buňky bychom tvarem mohli přirovnat k chobotnici, jeden výběžek může dosahovat délky až jednoho metru, přitom samotná buňka bývá velikosti v průměru nepřesahující desetinu milimetru. Jednotlivé neurony mají, jak píše Karel Pstružina a Oliver Tenzer /15/, schopnost vytvářet spojení a působit na jiné, i hodně vzdálené buňky, pomocí zvláštních výběžků neuronů, tzv. synapsí. Těmito spojeními vytvářejí velice složité a dynamické struktury, každá mozková buňka bývá spojena s jedním až pěti tisíci dalšími neuronovými buňkami.

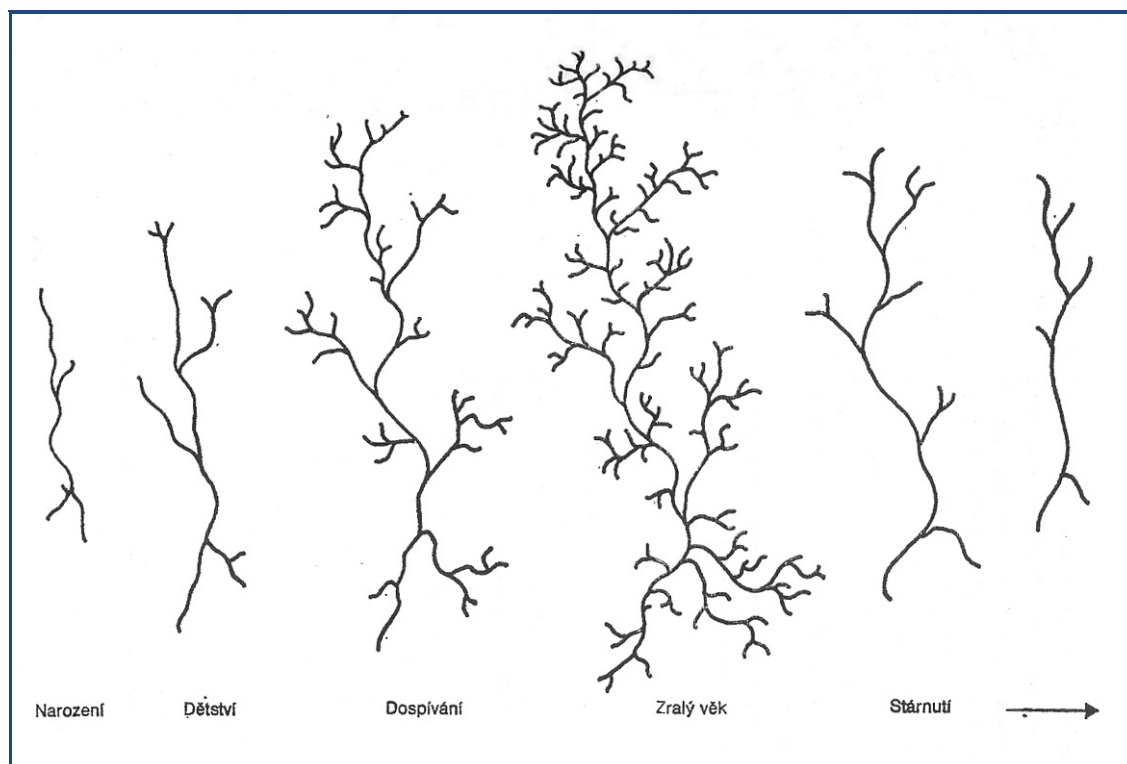
Dráždivost nervových buněk, jako jedna z jejich nejdůležitějších vlastností, ale není samovolná. Vzruch vzniká až po dosažení určité hranice dráždění, nějaké mezní hodnoty. Mohli bychom zde tedy najít jistou kontinuitu mezi činností nervových buněk a základním stavebním prvkem počítačů – tedy jedničkou a nulou, buď vše, nebo nic. Ale nemůžeme jen tak srovnávat lidský mozek a celou nervovou soustavu s počítačem, hlavně mají odlišné, dalo by se říci, pracovní prostředí. Zatímco nejvýkonnější počítače pracují stále jen na elektronické bázi, v mozku probíhá neskutečné množství chemických a biochemických operací. Celá jeho činnost je nesmírně dynamická, živá.

Jak poznamenává pan Cejpek v jedné ze svých publikací /4/, neurony se opravdu chovají jako živé organismy. Na tytéž podněty reagují při různých situacích různě. Jsou schopny učit se ze zkušeností, a proto na opakující se podněty mohou reagovat buď tím, že je přestanou vnímat, anebo naopak tím, že na ně budou reagovat stále citlivěji a tyto „cesty po neuronových drahách“ se stanou více využívanými. Tím dochází k samovolnému větvení často používaných synapsí, mění

svůj tvar, zakřivují se, zesilují, aby umožnily snadnější průchod vzruchů. Naopak synapse málo využívané postupně degenerují.

Aby mozek byl vůbec schopen reagovat na nějaké podněty, potřebuje k tomu energii, konkrétně ATP (adenozintrifosforečná kyselina). ATP se přitom tvoří z glukózy za přítomnosti kyslíku, proto jsou kyslík spolu s glukózou velmi důležité pro lidský mozek. Dokonce Karel Pstružina /15/ uvádí, pokud by do mozku nebyl dostatečný přísun kyslíku po dobu větší než 6 minut, dochází k takovým poruchám mozkových tkání, které už nelze obnovit.

V souvislosti s častým používáním frekventovaných neuronových spojení si člověk vytváří určité postupy, které si během života stále víc a víc osvojuje natolik, až se stanou rutinními. Například lidská chůze. Po prvních krůčcích následují další a další, chůze se stává stabilnější, jistější, plynulejší. Nejprve, když se malé dítě učí chodit, musí při každém kroku „zapínat a vypínat“ neskutečné množství neuronů v daném pořadí tak, aby postupně řídilo a koordinovalo své svaly a pohyby. Postupně se ale cvičením tohoto stejného postupu celý proces zautomatizuje tak, že už nemusíme naše pohyby vědomě ovládat a chůze se stane zcela přirozenou. Píše o tom i pan Pstružina /15/, že v časové perspektivě lidského života počet jednotlivých vazeb (synapsí) nejprve roste, ale pak se omezuje a upevňuje (znázorněno na obrázku 2.2).



Obrázek 2.2 - Vývoj neuronových struktur (převzato z /15/)

Co nám ale dává schopnost osvojit si určité postupy, metody, natolik, abychom je mohli provádět bez vědomého přemýšlení o nich? Tato schopnost se nazývá paměť, která dokáže uchovat informace v idealizované podobě, a znovu je poté řízeně vyvolat, ať už se jedná o jednoduché stavy nebo činnosti, tak i o složité struktury a vztahy. Někdy k opětovnému vyvolání námi chtěné informace může postačit návrat na určité místo, nebo návrat ve vzpomínkách k určité události. Stejně tak se můžeme pokusit o jakousi rekonstrukci, postupně z malých nepatrných střípků vzpomínek vytvářet celkový obraz.

Schopnost uchovávat a znovu opakovat stavy, činnosti, informace, je dána genetickou povahou, tedy dědičností, ale i samotným učením se. Čím více budeme mozek trénovat, tím nám bude lépe sloužit. Můžeme si to uvést na jednoduchém příkladu dvou mladých chytrých lidí po maturitě. Jestliže se jeden z nich rozhodne jít studovat na vysokou školu a bude se tomu opravdu věnovat, neměl by být pro něj velký problém toto studium zdárně dokončit. Pokud by ale stejně nadaný druhý člověk zvolil za svou nejbližší budoucnost práci, například hodně manuálně náročnou, patrně nebude mozek po dobu pracovního poměru tak zatěžovat, jako

člověk studující. Pokud by se poté tento pracující rozhodl přeci jen studovat, najednou zjistí, že už mu nestačí přečíst si probíranou látku pouze jednou nebo dvakrát, zjistí, že už to pro něj nebude tak snadné, jak by mohlo být, kdyby šel studovat hned po střední škole.

U některých lidí převládá mylný názor, že inteligence a schopnost učit se nové věci závisí na velikosti lidského mozku. Mozek člověka dosahuje většinou průměrné váhy kolem 1200 až 1400 gramů, ale váha, neboli velikost mozku, opravdu není tím faktorem, který by určoval, zda bude daný jedinec inteligentní nebo nikoliv. Příklady takovýchto lidí, kteří jednoznačně tuto mylnou domněnku vyvracejí, uvádí i kniha Svět moderního myšlení /15/, že jsou známy případy doslova imbecilů, kteří měli obrovský mozek, a naopak geniálních jedinců s mozkem malým. Konkrétně největší mozek měl dosud váhu 2870 gramů, a nepatřil rozhodně člověku inteligentnímu, právě naopak. Na čem tedy závisí, zda jsme schopni se učit a obohacovat naše vědomosti? Jednak na našich rodičích, neboť určité prvky geniality či nějaké konkrétní schopnosti se mohou dědit z generace na generaci, a jednak na naší výchově. Proto i když se narodí dvě děti se stejně velkým mozkem, neznamená to, že budou v životě stejně úspěšní, stejně chytří, stejně nadaní. Každý jedinec je svým myšlením unikátní, nenapodobitelný.

2.4 Význam jedinečnosti (osobnostního fondu) každého člověka

V mnoha velkých firmách se při ucházení o významnou pozici můžeme setkat s různými formami psychologických testů, které by měli odhadnout naši osobnost. Nejedni personální pracovníci se pak rozhodují na základě takovýchto testů, protože chtějí do své firmy takové typy lidí, které právě co nejvíce přebují.

Každý člověk je jedinečný svým osobnostním fondem, tedy jeho vnitrem, způsobem jak přemýšlí, jak chápe, jak si informace vybírá, které si zapamatovává a které ne. Osobnostní fond bychom mohli chápat jako naše dosavadní zkušenosti, znalosti, prožitky. Do lidského mozku vstupuje neskutečné množství různých podnětů, ovšem člověk není ani schopen na všechny reagovat, všechny si

uvědomovat. Většinu těchto podnětů nevnímáme, dochází tedy, dalo by se říci, k určité selekci toho, co přejde z této nevědomé oblasti do vědomé. Svým způsobem si tedy vybíráme, které informace si uchováme, osvojíme. A právě tato selekce je ovlivňována dosavadním životem člověka, jeho osobnostním fondem, vůlí a schopností poznávat. Jestliže se naučíme během života vybírat si cílevědomě informace a následně je zpracovávat, ukládat do paměti, můžeme se ve vyspělejší věku pyšnit nadhledem, racionalitou, moudrostí.

V jedné z minulých podkapitol jsme si zmínily, že podněty přicházející do mozku jsou mozkiem zpracovány a výsledkem tohoto zpracování je poznatek. Poznatek můžeme chápat jako čistě individuální, jedinečný. Je to znalost, kterou si vytvoříme díky našemu osobnostnímu fondu, a právě takto získaný poznatek pak následně náš osobnostní fond ovlivňuje pro budoucí život. Každý jedinec může mít ze stejné události jiné poznatky. Jinak bude vnímat, co se přihodilo, bude mít různé pocity, mohou se nám vybavovat vlastní vzpomínky na něco souvisejícího. Klasickým případem může být například autonehoda nákladního automobilu s osobním. Řidiči nákladních vozidel pravděpodobně budou dávat toto neštěstí za vinu řidiči osobního auta, a naopak. Někdo si vzpomene na svou vlastní havárii, anebo na příbuzné, známé, které mají podobné zkušenosti. Jiný si jen spočítá, kolik by vyšla oprava těchto zničených automobilů v jeho soukromé opravárenské dílně.

Jak si člověk buduje svůj osobnostní fond, jak si ho obohacuje? Jak je psáno o pár řádků výše, do mozku proudí ohromné množství podnětů. Ale dochází k selekci, takže samotný objem těchto podnětů rozhodujícím faktorem není. Spíš je důležité právě to, které informace si vybereme, které si uchováme, osvojíme. V knize Jiřího Cejпка /4/ je na příkladu ukázáno, že opravdu na množství podnětů až tak nezáleží. Je zde popsáno sledování televize a používání internetu, což obě tyto aktivity výrazným způsobem zvyšují počet informací, které jsou nám předkládány oproti minulým desetiletím. Ale dovolit si tvrdit, že dnešní lidé jsou chytřejší, vzdělanější, to opravdu nemůžeme. To, jestli budeme mít bohatší osobnostní fond, záleží na našich schopnostech a na naší vůli chtít z tohoto rostoucího světa zaznamenaného a distribuovaného poznání přiměřeně čerpat.

A právě s vůlí chtít něčeho dosáhnout, poznat nové věci, být vzdělanější, s tím vším souvisí učení. Doktor Nagel, zabývající se pedagogickou praxí a zejména hledáním, jak se chovat efektivně, ve své knížce /6/ poukazuje jak na některé

metody učení, jaké známe už delší dobu, tak i na novější hypotézy. Například metoda „Mind Map“ je velmi efektivní, je založena na tzv. klíčových konceptech, tematických okruzích, které nám zjednodušují přijímání nových informací. Učení bychom měli spojit s co největším množstvím pocitů a vnějších podnětů. Umět pracovat s asociací, přiřadit nové informace ke správnému klíčovému konceptu, znamená ukládat důležitá data v mozku blíže tematickému centru a tím je pak rychleji opětovně využít. S asociací pracovali už lidé v antickém Řecku. Pojem, který si chtěli osvojit, spojili s názornou představou nebo určitým symbolem. Dnes se této mnemotechnické pomůcky využívá pro lepší pochopení látky, posílení paměti a fantazie. Ovšem stále platí, že hodně studentů se učí pouze proto, aby uspěli u zkoušek, učí se celé věty nazpaměť, nehledají vzájemné vztahy. Nedokážou látce porozumět, pochopit ji. Kdekdo zná moudro, že celek je víc než jen součet jeho částí, tak proč se tím neřídíme? Proč se neučíme v souvislostech, a jen vysvětlujeme jeden pojem jinými, učíme se slovo od slova? Tím se zabývá relativně nová metoda síťového učení, která právě nabádá ke sloučení toho, co se učíme, s našimi pocity, přemýšlením, pochopením problému, porozuměním. Jen tak se můžeme stát vzdělanějšími, dokázat logicky uvažovat, správně odvozovat.

Celý proces učení ale probíhá už daleko dříve, než si vlastně sami dokážeme uvědomit, že se něco učíme. V dětství se přeci člověk naučí nejvíc za celou dobu jeho života. Velkou roli zde hrají rodiče a prostředí kde vyrůstá.

2.5 Vliv výchovy, sociálního a kulturního prostředí na individuálnost jedince

Nejen v dětství platí, že učení hrou je nejlepší způsob, jak si osvojit kdejaké zákonitosti tohoto světa, ale právě v dětství je toto nejdůležitější, vytváříme si návyky jak se vlastně učit, obohacujeme se o nové poznatky, které ovlivní náš budoucí život. Znamená to učit se bez stresu, bez donucení, mít z učení radost, bavit se při tom a přirozenou zvědavostí docházet k novým znalostem, poznávat širší souvislosti. Vše je tedy závislé na výchově, rodičích. Zdálo by se, že všichni jsme při narození na stejné startovací čáře, ale pravda to není. Každý se totiž rodí do

jiného sociálního prostředí, bude vychováván jinými metodami, ovlivněn jinou kulturou. Z toho pak pramení rozdíly mezi lidmi. V životě nezáleží jen na vrozeném talentu, ale i na odhodlání, snaze, na tom, jaký člověk je ve svém nitru.

Jak již je uvedeno v jedné předešlé podkapitole, různí lidé reagují na určité podněty různě, přisuzují datům odlišné významy, používají odlišné metody jak potřebné informace hledat. Zmínili jsme pro příklad výběr vhodného filmu ve večerním programu kina. Kdybychom si to zkusili trochu rozebrat, znamenalo by to, že postavíte-li vedle sebe dvě naprosto odlišné osoby, jejich výběr bude rozdílný. Pro ukázkou, zkusme si představit mladou dívku, žijící celý život v romantické představě okouzujícího rytíře na bílém koni. Byla vychovávána v harmonické rodině, kde láska k druhému znamenala více než peníze na nové šaty. O pár metrů dál si čte program úspěšný manažer středně velké firmy s velkými ambicemi na ředitelské křeslo. Vychovával ho otec, který ve dne pracoval a v noci popíjel, a matka, která na něj neustále neměla čas. Který film si asi vyberou? Myslím, že většina z nás se shodne na tom, že pravděpodobně nenavštíví stejný snímek. Mladá žena bude nejspíše vybírat romantickou komedii, ovlivněna svou výchovou, svými ideály. Bude se rozhodovat spíše podle rozmanitosti zápletky a jistoty šťastného konce, popřípadě podle obsazení sympatickými herci. Ale co sebejistý a cílevědomý manažer jdoucí se odreagovat od celotýdenního stresu z práce? Spíše zvolí jistotu ve formě napínavé podívané plné tajuplných zauzlení, intrik, podvodů a zbraní. Proč se každý rozhodl pro naprosto odlišný film? Protože vyrůstali v rozdílných sociálních poměrech, působilo na ně jiné kulturní prostředí, vnímají svět okolo sebe jinak, rozhodují se jinak, chovají se jinak. Výchova člověka značně ovlivňuje v tom, jaký bude v dospělosti. Zde, ve výchově, pramení tolik odlišností mezi lidmi. Jedni mohou celý život bojovat za lepší životní prostředí, druzí se budou snažit z přírody vytěžit a doslova vyždímat co nejvíce, jen aby z toho měly prospěch.

3 Informace jako základ lidského jednání a rozhodování

3.1 Člověk jedná v závislosti na informacích

Měli bychom si uvědomit důležitost správných informací při určitém rozhodování, protože bez informací a znalostí se neobejdeme, pokud chceme řešit situace co nejefektivněji. Na dalších řádcích si na příkladech ukážeme zajímavé srovnání dostatku informací dříve a dnes při rozhodování, současné projekty se totiž řeší i s využitím dřívějších zkušeností, ale i chyb a omylů.

Veškeré jednání člověka, ať se jedná o relativně banální záležitost každodenního života, nebo o důležité rozhodnutí, které může změnit chod celé firmy, je ovlivněno mírou informovanosti daného jedince. Záleží, jaké má informace o dané problematice, kterou musí řešit. Jestli jsou dostačující, relevantní. Před samotným hledáním východisek si musíme položit čtyři základní otázky, abychom věděli, máme-li se daným problémem vůbec zabývat. Jedná se o jednu z metod systémové metodologie, tzv. Occamovu břitvu. Ptáme se, zda se vlastně daný problém týká nás? Máme dostatek relevantních informací, popřípadě, jsme schopni si je v rozumném časovém intervalu opatřit? Dokážeme problém vyřešit v rozumném čase? Chceme ten problém vůbec řešit? Otázky o informacích jsou nesmírně důležité, pokud bychom neměli dostatek informací, respektive relevantních informací, nemusí být námi navrhované řešení správné.

3.2 Nutnost získávání informací

Jak píše Kurt Nagel /6/, každé lidské jednání je provázeno stálým hledáním správných rozhodnutí. Téměř vždy se rozhodujeme s určitou mírou rizika a na kvalitě rozhodnutí může záviset i úspěch celé organizace. Proto by měl každý vědět, jak se rychle a s minimální mírou rizika správně rozhodovat. Ale pro mnoho lidí je velmi obtížné správné rozhodnutí nalézt. Důvodů uvádí několik. Lidé neznají

podstatu problému, rozhodují se podle naučeného vzorce, neznají kritéria cílů a rozhodnutí, uvažují o malém počtu alternativ, rozhodují se pod časovým tlakem, a v neposlední řadě nemají všechny potřebné informace. A právě tomuto poslednímu důvodu bychom měli věnovat pozornost, naučit se ho co nejlépe eliminovat.

Získávání informací je jednou z nejdůležitějších činností mnoha firem a institucí. V posledních letech a desetiletích rostou počty informačních center. Informační aktivity totiž leckdy přinášejí podnikatelům větší zisky než samotná činnost podnikání. Proto i roste počet lidí pracujících v takovýchto informačních střediscích, kteří získávají a poskytují informace. Často stojí vznik takovýchto pracovních pozic v podnicích nemalé peníze, ale jejich návratnost při správné aktivitě v práci s informacemi bývá několikanásobná. Je to logické, protože právě správné informace jsou leckdy klíčem k úspěchu celé organizace. Informace jsou důležité ve všech fázích podnikání. Například v marketingovém oddělení musejí přesně znát, na který trh se bude společnost koncentrovat, nebo jaké mají zákazníci požadavky na kvalitu zboží, ale třeba i na obal a barvy. Při vyhodnocování finanční situace je nezbytné znát finanční a daňové zákony příslušné země, možnosti pořízení půjčky od bank atd. Při samotné výrobě a distribuci zboží je nezbytné provádět průběžné kontroly, jak je daný výrobek prodáván, jestli se vyplatí pokračovat ve výrobě nebo se soustředit na jiný produkt. Potřeba informací je tedy opravdu nezbytná, životně důležitá pro správné fungování.

Ovšem stejně jako v životě platí, že někdy méně znamená více. Přemíra informací totiž naši schopnost rozhodování ztěžuje, nejsme schopni si vybrat ty podstatné, ty, které opravdu potřebujeme. Jinými slovy je důležité vědět, co nečíst, nestudovat. Nejefektivnější práce s informacemi je ta, při které vybíráme jen ty, které se pro náš úkol nejlépe hodí. Musíme ale také umět rozlišit, zda je získaná informace pravdivá, spolehlivá. Nedůvěřivé informace mohou být dokonce velmi nebezpečné. Vladimír Smetáček to ve své knize /12/ ukazuje na příkladu, kdy člověk zakoupí určitou potravinu na základě inzerátu, který ji prohlašuje za zdravou výživu. Ovšem pokud je inzerát nepravdivý, a výrobek nám bude škodit, ztratili jsme jak peníze, tak zdraví.

Proto ne každý by se hodil na takovou práci, kdy musí získávat a zpracovávat informace. Tato činnost je velice individuální a záleží na vnitřních dispozicích každého jedince. Ti, kdo mají výbornou paměť a dokážou logicky přemýšlet a

uvažovat, si většinou vystačí jen s novými fakty, kdežto lidé s horší pamětí musejí pokaždé hledat vše znova. Dalším úskalím v lidském faktoru při práci s informacemi je, že mnohokrát mají lidé pocit, že ví jakým způsobem řešit určitou situaci, a proto mají dojem, že vlastně žádné nové informace nepotřebují. Ale leckdy to bývá pocit mylný. Kdyby management dnes úspěšné firmy nezískával průběžně nejnovější informace o technickém pokroku, kterého využívají jeho konkurenti při zlepšování své pozice na trhu, nebude už za pár let konkurence schopný. To, co se nám dnes jeví jako nejlepší řešení, nemusí být tím nejlepším po celý výrobní proces po několik let. Proto bychom se měli vždy snažit hledat dostatek informací, které budou pro nás a pro naše jednání užitečné. Každý problém, před kterým stojíme, důkladně zanalyzovat a promyslet ze všech stran, abychom pak dokázali co nejefektivněji nalézt takové informace, které skutečně potřebujeme.

3.3 Na co si dát při hledání informací pozor

Často se setkáváme s problémem, že námi získané informace, které jsme tak dlouho hledali, jsou zastaralé, nepoužitelné. Informace stárnou velmi rychle, v některých oborech více, v jiných méně. Stále ale platí, že bychom se měli snažit hledat informace co nejnovější, nejpřesnější. Na základě starých informací se nám nepodaří vymyslet nejlepší, nejoptimálnější řešení, lidé s novějšími informacemi budou vždy o krok napřed.

Ale zastaralost není jediným problémem, který se může objevit při práci s informacemi. Vladimír Smetáček /12/ uvádí celkem čtyři důvody, proč může být získaná informace chybná. Jednak je to již zmíněná zastaralost informací, tedy fakt, že další výzkum zjistil poznatky, které dosavadní informace vyvracují. Další chybou je, pokud informace vyjadřují chybný poznatek, který je však všeobecně uznáván jako správný. V těchto případech je téměř nulová možnost zjistit bez vlastního prozkoumání, že je daná informace mylná. Třetí případ se vyskytuje, když dojde k chybě při zpracování a komunikaci informace. Tyto chyby se nejčastěji vyskytují ne v oficiálních informačních zdrojích, ale například v běžné řeči při setkání s neformálními zdroji, kdy slyšíme slova „říká se“, „prý“ a podobně. Nejhorší však

může být situace, kdy je chyba vytvořena záměrně, hovoříme pak o tzv. dezinformaci, jejímž účelem je poškodit nepřítele, konkurenta. Dezinformace se neobjevují jen v oblasti špionáže a vojenství, ale i v obchodu a průmyslu.

Rozhodně tedy platí, pokud budeme mít pochyby o nějaké informaci, zkusit si ji co nejvíce prověřit, nespoléhat pouze na jeden zdroj, nedůvěřovat na sto procent žádné informaci a pokusit se ověřit si ji z více pramenů. Mohlo by se nám pak stát, že na jejím základě učiníme rozhodnutí, které se posléze ukáže jako mylné.

Hodně probíraným tématem je cena informací. Ne vždy platí, že co je drahé, to je dobré. Ale je zřejmé, že nové informace stojí dost peněz, když se získávají třeba ze zahraničních pramenů. Ale pokud je informace pro firmu prospěšná, investice se jistě vyplatí. Takové informace mají cenu úměrnou případnému zisku, užitku, prospěchu z dané informace. Čím výnosnější je informace, tím víc nás bude stát. S otázkou peněz ale bohužel úzce souvisí různé podvody. Setkáváme se situacemi, kdy firma za úplatu získá velmi ceněnou informaci, například kudy povede nová dálnice, a v těchto místech vykoupí pozemky za ceny ještě relativně nízké. Po té, co informace prosákne na veřejnost, cena takovýchto pozemků rázem stoupne i na několiknásobek původní hodnoty. Firma pak může profitovat jak ze zpětného prodeje, tak i z možnosti výstavby vlastních motelů a restaurací.

Abychom se vyhnuli zbytečnému peněžnímu výdaji, musíme si nejprve uvědomit, zda danou informaci opravdu potřebujeme, a hlavně, jestli ji dokážeme využít. I kdybychom měli možnost získat sebelepší informaci, pokud ji nebudeme schopni využít a přeměnit ji tedy nějakým způsobem v náš prospěch, je zbytečné za tuto informaci platit. K čemu by nám byla drahá informace o fungování nejlepšího mobilního telefonu, který zrovna vynalezli inženýři v Japonsku, když pro jeho provoz ještě několik let nebudou v naší republice možnosti? Jak je psáno výše, záleží na individuálních schopnostech každého člověka, který se zabývá pracemi s informacemi, aby vyhodnotil, která informace je pro nás přínosná, důležitá.

3.4 Rozdílnost řešení projektů na základě informovanosti

Lidé stojící před závažným rozhodnutím potřebují znát co nejvíce informací týkajících se daného problému, aby je mohli analyzovat, zhodnotit a následně zvážit, jaké rozhodnutí bude to nejlepší. Pro někoho může být oním závažným rozhodnutím nákup nové postele, pro jiného výběr vhodné parcely k postavení nového závodu. Zkusme si nyní jeden tento hypotetický příklad představit. Jak by asi jednali lidé, mající dostatek informací, a lidé, kteří se rozhodují podle toho, co jim řeknou obchodníci? Člověk racionálně uvažující si před koupí nové postele získá informace, jaké jsou vlastně typy postelí na trhu, z jakých jsou materiálů a jaké druhy matrací se dají sehnat. Poté si rozmyslí, co z nabízených postelí by vyhovovalo jeho potřebám a zjistí si také ceny u více prodejců. Pak se může s klidem rozhodnout, jakou postel si vybere. Ale člověk, nemající zájem si něco zjišťovat, člověk, který postelím a matracím nerozumí a jde mu hlavně o to mít nějakou postel, zajde do prvního obchodu, který je nejbližší, a tam se nechá nalákat prodejcem ke koupi postele, kterou třeba původně vůbec nechtěl. Který z nich je více spokojený? Samozřejmě že ten první, ovšem musíme se ještě pozastavit nad získáváním informací. Všeobecně by mělo platit, že mezní náklady na získání potřebných informací mají být menší než přínos z informací, respektive z rozhodnutí založeného na těchto informacích.

Rozdílnost informovanosti je však nejlépe patrná na projektech, které řešíme dnes, a na těch z minulých let, desetiletí, století. Dříve nemohli lidé používat počítače na vykreslení 3D modelů ještě před samotným zahájením stavby, museli se spolehnout na vlastnoruční nákresy. Dnes s využitím moderních počítačů jsme schopni určité činnosti, co dříve trvaly hodinu, realizovat za zlomek původního času. V tom je velká výhoda dnešní doby. Jednak víme, jakých chyb se dopustili lidé v dřívějších dobách a můžeme se z nich poučit. Dále pak už také známe určité zaručené metody jak postupovat. Všechny dřívější projekty pro nás představují nepřehledné množství informací, které můžeme zužitkovat. Navíc, jak již je psáno výše, dnes pro nás informační a komunikační technologie znamenají ohromné zrychlení a zefektivnění práce. Ať už jde o velký stavební projekt, nebo o výuku cizích jazyků, kdy můžeme využít mnoha a mnoha výukových počítačových programů.

Se zdokonalováním technických zařízení, novými výrobními stroji i moderními počítači, se mění i samotný význam informací. Jednak se mění jejich podoba, před pár stoletími by asi nikdo nevěděl, co máte na mysli, pokud hovoříte o informaci v elektronické podobě. Stále více a více je důležité vynakládat prostředky pro získávání informací, jejich vliv na úspěch v dnešní době je značný. Už byla řeč o rostoucím počtu informačních center a o nárůstu pracovních míst v takovýchto oborech. Je to logickým vyústěním rozšířeného zájmu o informace, potažmo o dobrou konkurenci schopnost, kvalitní výrobky, efektivní rozhodování.

Když jsme zmínili řešení projektů dnes a v minulosti, přiblížíme si to například na mezinárodním letišti v Hong Kongu. Určitě každý z Vás si dokáže vzpomenout na nějaký obrázek starého letiště Kai Tak, které se nacházelo přímo uprostřed této rušné metropole v jihovýchodní Asii. Jak píší internetové stránky SkyFliers /10/ a /9/, letiště bylo obklopeno mrakodrapy a zejména vysokými horami, které letadlům znemožňovali normální přiblížení. Každé přistání se stalo nervy drásajícím zážitkem jak pro piloty tak pro cestující. Letadla létala těsně nad střechami mrakodrapů a mířilo přímo na vysokou horu, až v posledním okamžiku muselo prudce stočit doprava a dosednout na ranvej vybudovanou na přístavní hrázi. Několikrát se i stalo, že letadlo skončilo přímo v moři.

Ovšem když se toto letiště stavělo, zdála se vybraná lokalita nejvhodnější. Nebyly k dispozici ještě informace, které už měli inženýři před patnácti lety, kdy se rozhodovalo o vybudování nového, modernějšího a bezpečnějšího letiště. Necelých 40 kilometrů západně od centra velkoměsta byl vybudován umělý ostrov Chep Lap Kok, kdy půda původního malého ostrůvku se rozhrnula, díky mnoha kilogramům výbušnin se podařilo srovnat se zemí všechny kopce a vznikla prostorná a rovná plocha ideální pro nové letiště. Celý velkolepý terminál je pod jednou střechou. A právě při této stavbě se využilo mnoha a mnoha informací z podobných projektů v minulosti. Samozřejmě, používání trhavin je známé už delší dobu, ale možnost malý kopcovitý ostrůvek změnit v pevnou rovinu čtyřikrát větších rozměrů, to už tak obvyklé není. Samotný terminál byl také vybudován s použitím informací z dřívější doby. Konkrétně se jednalo o londýnské letiště Stansed, které se stalo takovým vzorem, nebo alespoň inspirací, pro tento na světě největší zastřešený uzavřený veřejný prostor. Nebýt informací získaných z dřívějších mnoha a mnoha stavebních projektů, asi by nové letiště nevyrostlo a nenahradilo staré,

v posledních letech své existence už zcela nevyhovující, letiště. Zde je tedy vidět rozdílnost rozhodování, pokud určité informace známe, nebo ne. Mít v době výstavby starého letiště informace, které známe dnes, patrně by už tenkrát vyřešili potřebu velkého mezinárodního letiště lepším způsobem.

4 Zdroje informací, odkud čerpáme dnes a odkud v minulosti

4.1 Kde začínáme hledat informace

Abychom mohli využívat znalostí jiných lidí, musíme vědět, kde tyto informace hledat. Vše, co kdy bylo vynalezeno a co se používá, je někde zaznamenáno. Zkusíme si tedy přiblížit, jaké máme možnosti při hledání informací.

Nemusíme ale informace čerpat pouze z cizích zdrojů, ale i z vlastní paměti. Vladimír Smetáček /12/ o vlastní paměti píše jako o nejlépe dostupném informačním systému, aniž si to uvědomujeme, vždy hledáme právě nejdřív v ní. Ovšem cílem informačního systému není jen informace uchovávat, ale především je znovu nalézt. Zde autor připomíná dvě nepříjemné vlastnosti paměti. Jednak si řadu věcí zasuneme do pozadí, takže buď ani nevíme, že je známe, nebo tušíme, ale nedokážeme si vzpomenout. Druhým problémem je zkreslování, které spojí prvky z různých oblastí a tím nám poskytne velmi nepřesné až zavádějící informace. Proto krom rutinních případů nemůžeme paměti vždy stoprocentně důvěřovat a musíme hledat informace jinde, popřípadě se ujišťovat v tom, že informace, které si pamatujeme, si pamatujeme správně.

Pokud tedy chceme jen ověřit platnost našich informací získaných s vlastní paměti, stačí leckdy pouze kontakt se známými, s přáteli, nebo s odborníky. Ovšem musíme si zvolit ty správné známé a přátele, může se totiž stát, že i oni budou považovat nějaké údaje za správné a poté se ukáže, že jsme se mýlili všichni. U odborníků, pokud volíme tedy experty z dané oblasti, která se týká informací, jež potřebujeme ověřit, by takovýchto situací mělo být po málu. Zde je ale zase někdy potřeba počítat s určitým peněžním výdajem za odbornou radu.

4.2 *Prapočátky sdělování informací*

I v dobách vzdálených mnoho století, ba i tisíciletí, existovaly informace, které si lidé potřebovali vyměňovat. Například aby našli správnou cestu přes pohoří na cestě za hledáním nového místa pro přesídlení. Nebo aby i příští generace věděly, jak vyrobit nový nástroj pro lov zvěře. Nejprve bylo dorozumívání a tedy sdělování informací (podle definice, že informace je název pro obsah, který lidé komunikují) velmi primitivní. Pomocí kouřových signálů se sdělovali informace, že ten, kdo je vysílá, dorazil v pořádku, ulovil zvěře atd. Následně vznikaly jednoduché metody jak ukázat správnou cestu pomocí kamenů a větví, z kterých se dal na zemi vytvořit tvar šipky.

Jako prvopočátky písma můžeme označit staré kresby na stěnách jeskyní, později doprovázené piktografickými nápisy, tedy jakýmsi obrázkovým písmem, kdy se celá slova zobrazovala pomocí obrázků. Naskytl se tak lidem nový způsob, jak vyjádřit například své pocity, ale i jak popsat zvěře, se kterým se dosud nesetkali. Zaznamenávali informace, pomocí nichž lidé, kteří přišli později, věděli, jak vyrobit sekeru, luk, jak vypadá zvěře, které se zde vyskytuje a podobně. Ovšem snazší, než zaznamenávat informace pomocí obrázků znázorňující celé slova, je zaznamenávat každé písmeno zvlášť. Nemusí pak docházet k nejasnostem, co daný obrázek představuje. Vzniklo tedy písmo hláskové.

4.3 *Nosiče informací*

Vznik písma s sebou přinesl i první knihy, respektive nejprve hliněné destičky, papyrus a pergamen. První kniha z papíru byla vyrobena až ve 14. století, a rok 1450 snad v souvislosti s knihou není třeba nikomu vysvětlovat. Jen pro připomenutí, vynález knihtisku výrazně rozšířil možnosti sdělování informací, už nemusely desítky lidí přepisovat ručně dlouhé a dlouhé dny jednu informaci, díky knihtisku se její zaznamenání urychlilo a mohla být i dostupná více lidem.

Jiří Cejpek /4/ uvádí, že na konci 19. století se jako hmotný nosič, na němž nebo do něhož jsou znakově zaznamenány znalosti či zkušenosti, tj. potencionální

informace, se začíná používat označení „dokument“. Knihy, respektive dokumenty, výrazně zlepšily zprostředkování výsledků lidské práce ostatním prostřednictvím knihoven a knihovních služeb.

Ovšem kniha není jediným typem dokumentu, můžeme ji označit jako dokument textový, tedy tištěný nebo psaný projev. Rychle se rozrůstající počet textových dokumentů s sebou přinesl vznik knihovnictví, dokonce i jako studijního oboru. Pan Cejpek uvádí, že vznikla i knihovní věda, která se zabývá komunikací textových dokumentů v knihovnách. Pro optimalizaci vyhledávání se vytvořilo mnoho indexačních a pořádacích systémů. Jedná se o metadata, tedy data o datech, které popisovaly dokumenty z různých hledisek. Jazyk používaný pro zápis do rejstříku byl například ochuzen o citově zabarvená slova, musel co nejpřesněji a nejjednodušeji vystihovat, o čem daný dokument vypovídá. Právě vytvoření takovýchto katalogových souborů je klíčem k tomu, aby se z hromady knih stala uspořádaná sbírka knih, tedy knihovna.

Nemusíme ale informace čerpat jen z knih, s rozvojem technického pokroku vznikly i další typy dokumentů, z kterých se můžeme dozvědět to, co potřebujeme. Jedná se o auditivní a audiovizuální dokumenty. Auditivní dokumenty jsou určeny ke sdělení informací pomocí poslechu záznamu. Audiovizuální pak obsahují kromě zvuku i obraz. S rozšířením těchto dvou typů dokumentů se i rozšířily možnosti knihoven, mohou zákazníkům poskytovat informace přesně podle jejich představ.

Počítač s sebou přinesl dokumenty digitální, které mohou být dnes pomocí internetu přeneseny z jednoho místa na druhé, i na tisíce kilometrů vzdálené, ve velmi krátkém čase. Dostáváme tedy možnost získat informace z druhého konce světa během pár vteřin. Můžeme tvořit nové a nové digitální kopie, aniž bychom nějak snížili kvalitu, dokonce ani nemusíme poznat rozdíl mezi kopií a originálem. Digitální dokumenty tedy mají v sobě ohromný potenciál a využívají se stále více a více jako zdroje informací.

4.4 *Tištěné zdroje informací*

Jako tištěné zdroje informací dnes můžeme použít například knihy, časopisy, letáky, plakáty, atd. Velké množství takovýchto dokumentů uchovávají knihovny. Ovšem knihovny nevznikly až po objevu knihtisku, ba naopak. Existují zde už od dob nám hodně vzdálených. Za nejstarší nám známou knihovnu se považuje knihovna posledního vládce Asýrie, krále Aššurbanipala v 7. století před naším letopočtem. Slavnějšího jména se dočkala pak Knihovna Alexandra Velikého, ve které prý bývalo uchováváno až 700 tisíc svitků. Jak je napsáno výše, dnešní knihovny už ve svém fondu nenabízejí jen knihy, ale dokumenty nejrůznějších druhů, proto o knihovnách můžeme mluvit i jako o mediátekách. Navíc dnes jsou knihovny vzájemně mezi sebou propojeny a tak není problém získat, díky meziknihovní spolupráci a knihovním sítím v celosvětovém měřítku, nějaký dokument, který může být uložen na druhém koutě republiky, nebo i v jiném státě. Řada knihoven nabízí své katalogy k prohlížení na internetu, uživateli tedy stačí vyhledat si danou publikaci, zarezervovat si ji a pak už si počkat, až mu přijde oznámení, že si ji může vyzvednout na jemu nejbližší pobočce. Práce s informacemi se tak stává rychlejší, efektivnější. Nemusíme už cestovat napříč státem, abychom navštívili jedinou knihovnu, kde se daný výtisk vyskytuje, a zjistili, že je zrovna vypůjčený. I na tomto příkladě je vidět, jak informační a komunikační technologie výraznou měrou přispívají k lepší informovanosti a k lepší dostupnosti informací.

Pokud se bavíme o knihovnách, bylo by vhodné alespoň ve stručnosti zmínit některé významné knihovny současnosti. Co se týká České Republiky, největší je Národní knihovna v Praze. Vladimír Smetáček /12/ popisuje jako její hlavní činnosti především shromažďování bohemik, tedy knih a dalších dokumentů, které byly napsány Čechy, byly vydány na území českých zemí nebo se týkají Čechů a české problematiky. Dále Národní knihovna obstarává metodické řízení všech knihoven na území České republiky, funguje jako centrální místo v systému meziknihovní výpůjční služby a shromažďuje veškeré odborné knihovnické a informatické literatury.

V celosvětovém měřítku je největší knihovnou Kongresová knihovna USA (Library of Congress) ve Washingtonu. Byla založena roku 1800 a původně měla sloužit jen pro samotný kongres, ale během let rozšířila své služby až do dnešní

podoby národní knihovny. Kvůli nárůstu dokumentů, které spravovala, musela být dokonce přestěhována z původní budovy Thomase Jeffersona do dvou rozlehlejších. V současné době obsahuje více jak 100 milionů položek a stala se i lépe přístupnější pro uživatele díky online katalogu.

Mnoho lidí přichází do knihoven bez toho, aby měli přesnou konkrétní představu o tom, z jakého oboru jsou informace, které požadují, kde je hledat a podobně. V takovýchto případech nám pomáhají pracovníci knihoven, jejichž práce se s vývojem knihovnictví výrazně změnila. Z dřívější knihovnické praxe se stalo podle Jiřího Cejpky /4/ odborné povolání. Tento zlom nastal na konci 19. století, kdy ve Spojených státech amerických byla založena první knihovnická profesionální organizace na světě, American Library Association. O pár let později, konkrétně roku 1887, vznikla první knihovnická škola na Columbijské univerzitě. Knihovnictví jako studijní obor je důležité pro odborný růst lidí, kteří se v budoucnu budou starat o to, aby naše požadavky po informacích byly co nejlépe uspokojovány. Nemusí se jednat jen o zaměstnance knihoven, ale i o tzv. informační manažery. Lidé zastávající tuto relativně novou profesi se orientují na celkovou informační architekturu podniku.

Knihovny jako takové dnes můžeme najít v každém větším městě, na některých středních školách a většině vysokých škol, kde jsou k dispozici mimo jiné i publikace učitelů dané vysoké školy. Ovšem instituce s charakterem knihoven vznikali i ve velkých výrobních podnicích. Plnily také funkci uchování a znovu zprostředkování informací. Hlavním důvodem k jejich zřízení bylo přiblížit informace co nejbližší k pracovišti, poskytnout uživatelům co nejrychlejší odbornou pomoc. Takovéto instituce ale v podnicích málokdy nalezneme pod označením knihovna, spíše se o nich hovoří jako o dokumentačních nebo informačních střediscích.

4.5 Elektronické zdroje informací

Elektronickými zdroji dat můžeme chápat jak již zmíněné dokumenty auditivní a audiovizuální, tak i dokumenty textové. Mnoho informací je uloženo ve zvukových záznamech, dokumentárních filmech a podobně. V televizních archivech, filmotékách, videotékách, ale i v knihovnách, existuje přemíra takovýchto dokumentů, které mohou být kdykoliv znovu a znovu přehrány a tím nám poskytnout údaje, které potřebujeme, které hledáme.

V posledním desetiletí se výrazně rozšířilo v naší republice používání počítačů a internetu. Počítače samy o sobě v sobě skrývají velké možnosti, jak získat informace například z CD-ROM nebo z disků DVD, na kterých se běžně dají sehnat nejrůznější výukové programy ať už pro základní školy, tak i pro starší lidi, kteří se chtějí sami naučit perfektně cizí jazyk. Výukové programy ale nejsou jediným zdrojem informací, který můžeme na kompaktních discích získat, hodně organizací poskytovalo své firemní informace a dokumenty právě prostřednictvím těchto médií. Dnes už převládá spíše používání internetu.

Internet, který se vyvinul v 60. letech z malého experimentu pro americkou armádu, Arpanetu, má dnes velmi široké spektrum použitelnosti. Počet počítačů, připojených do této celosvětové sítě, den za dnem narůstá, je to otevřená síť, do které se může připojit skoro každý. Na internetu dnes můžeme najít téměř jakékoliv informace, ovšem zde se naskytá otázka, zda je to dobře. Zda nemůže zvědavého školáka informace o výrobě jednoduché bomby natolik inspirovat, aby si to vlastnoručně vyzkoušel. Nicméně platí, že je to nesmírně pomocný nástroj moderní doby. Můžete během krátkého okamžiku získat informaci z druhé strany polokoule, pokud je v jazyce, kterému nerozumíte, můžete si ji přes internet nechat přeložit. Internet můžeme použít, i když chceme využívat řekněme klasických zdrojů informací, tedy knihoven. Přes online katalogy si můžeme vybrat nějaký dokument, zjistit, zda se zrovna nachází v knihovně, nebo zda ho má někdo půjčený. V tom případě si ho můžeme zarezervovat klidně z domova a počkat, až nám dorazí po schránky elektronické pošty oznámení, že je již pro nás připraven k vyzvednutí.

Internet je tedy vynikajícím pomocníkem současné doby pro práci s informacemi. Ale zároveň je to pomocník zatím nejnebezpečnější. Mnoho nalezených informací se nemusí zakládat na pravdě, mohou být získány podvodnou

činností. Právě ochrana dat na internetu je velmi důležitá, protože hrozba zneužití osobních údajů, nebo důležitých firemních informací, je velká. O bezpečnosti informací a ochraně dat proti zneužití bude ještě řeč v dalším textu. Dalo by se říci, že hrozba, kdy nám někdo odcizí informace, které sdílíme po internetu, je jakousi daní za možnost internet používat a profitovat tak z jeho předností.

Nicméně, na internetu se dá nalézt téměř cokoli. Vyhledávat informace zde můžeme pomocí katalogových souborů, vyhledávacích serverů nebo souhrnných vyhledávacích služeb. Předmětné katalogy usnadňují uživatelům hledání především pomocí třídění informací do jednotlivých kategorií. Naproti tomu vyhledávací servery umožňují vyhledat webové stránky podle textu, který je v nich obsažen. Používají při tom složitější vyhledávacího jazyku, který katalogy nemají. Souhrnné vyhledávací služby jsou pak, jak píše Jiří Bráza /3/, vyhledávací servery, které jsou schopny náš dotaz položit různým vyhledávacím serverům. Jako nejznámější souhrnnou vyhledávací službu na českém internetu autor jmenuje stránky www.alenka.cz. Používá také pojem metavyhledávače, což mají být vyhledávací služby, které vyhledávají u vyhledávačů a nikoliv v celém internetu.

Jak je vidět, internet nejen že je téměř nekonečným zdrojem nejrozmanitějších informací, nabízí nám i několik možností volby, jak v něm vyhledávat. Ale i přes tyto rozmanitosti, které nám internet přináší, stále existuje množství informací uložených v počítačových bázích dat, které ne vždy jsou z internetu přístupné. Vladimír Smetáček /12/ je dokonce rozděluje do tří kategorií. Bibliografické databáze, které obsahují informace o sekundárních pramenech k určité tematice. Dále pak referenční báze, které odkazují na určitá fakta, instituce, lidi, události a podobně. A nakonec faktografické databáze, které umožňují okamžité vyhledání konkrétní informace například o firmě, výrobku, technologii. Jak je vidět, elektronických zdrojů informací máme na výběr opravdu hodně.

4.6 *Ostatní zdroje dat*

Kromě knih, elektronických dokumentů a internetu, existují ještě jiné zdroje dat. Pravda, že v poslední době už nejsou tak využívány jako dříve, protože své informace mívají přístupné i z internetu, ale rozhodně je nesmíme opomíjet. Většina velkých organizací má své vlastní informační služby, které nám mohou při hledání správných informací pomoci.

Mezi takovéto organizace bychom mohli zařadit například státní správu, která se snaží vybudovat jednotný informační systém jak na úrovni ministerstev, tak i na úrovních jednotlivé místní správy, tedy obcí. Velice jsou využívány kontrolní orgány, které by měly upozorňovat na vývoj skutečnosti, přijímat podněty od obyvatelstva a reagovat na ně. Kromě státní správy by bylo vhodné ještě zmínit banky, jejichž informační systém by měl pomoci zákazníkům získat všechny potřebné informace například o poskytování úvěrů. Samozřejmě, že tyto informace jsou k nalezení i na internetu, leckdy je ale lepší osobní kontakt a zjistit si informace šité přesně na míru našim potřebám.

Ještě bychom do ostatních zdrojů informací, tedy nejrozumnějších organizací, mohli přidat i různé poradenské a konzultační firmy, popřípadě advokátní kanceláře. Poradenské firmy mívají obvykle velký rozsah činností. Dokážou začínajícímu podnikateli či novému podniku navrhnout vhodnou organizační strukturu, finanční plány a podobně. Pro firmy stojící na startovní čáře svého života tak poskytují vzácné informace, které jim mohou ušetřit spoustu nepříjemností, i peněz.

5 Ochrana proti zneužití informací

5.1 Bezpečnost je důležitá

Když získáme nějaké nové informace, nebo naopak chceme někomu informace poskytnout, musíme si dávat pozor, aby je žádná třetí strana nezneužila. Pokud jako zdroj informací volíme známé a přátele, nebo tištěnou literaturu běžně dostupnou z knihoven, používáme zdroje většinou veřejně přístupné, nehrozí tedy nějaký útok nepovolaných stran, aby je získaly také. Pokud se ale jedná o informace od expertů a odborníků, z tištěné literatury dostupné jen určitému okruhu lidí, nebo z elektronických zdrojů, pak už tato hrozba existuje. Stejně tak pokud chceme zprávu někomu sdělit, jedná-li se o něco důvěrného, měli bychom si dávat pozor na potenciální útočníky a volit co nejbezpečnější formy přenosu. Hovoříme tedy o špionáži, respektive snaze lidí získat tajné informace, většinou nelegální cestou, bez vědomí jejího odesílatele, příjemce, nebo tvůrce.

V knize Marka Lloyda /5/ je o špionáži pojednáváno jako o nejstarší, nepřitažlivější a nejtrvalejší lidské činnosti. Špionáž existuje už mnoho a mnoho staletí, dokonce o potřebě špiónů psal před 2400 lety i čínský vládce z doby Konfucia, který je dosud ve vojenských kruzích studován. Potřeba získávat důležité informace, které nejsou jen tak volně přístupné, existuje odnepaměti. Například i japonští ninjové z 12. století byli trénováni, aby mohli pracovat v co nejlepším utajení a tak co nejvíce nepozorovaně získat určitou informaci. Mark Lloyd /5/ se zmiňuje i o tzv. Černém kabinetu, který vznikl díky kardinálu Richelieumu. Za úkol měl zachytávat a analyzovat korespondenci francouzského dvora a nižší šlechty a přispěl tak velkou měrou k setrvání Ludvíka XIII. na královském trůnu. V 16. století pak Ivan Hrozný, první moskevský kníže korunovaný na cara, zřídil první ruskou politickou policii, tzv. Oпричину, která byla stejně krutá jako její vládce a jejím posláním bylo nalézt a vypátrat každý náznak zrady. Na konci 19. století se pak první vládní špionážní agenturou ve Washingtonu stala kancelář pro námořní rozvědku, která shromažďovala a evidovala informace ze sféry vojenského námořnictva pro potřeby ministerstva v době války i míru.

V minulém století se pak hodně často začala zmiňovat průmyslová špionáž. Tedy snaha získat od konkurenční firmy důležité a tajné informace, například údaje o zařízení, plány výrobního procesu a podobně. Vznikala celá řada špionážních zařízení a postupem času se změnily i nejpoužívanější techniky podvodného získávání informací, od například miniaturních fotoaparátů nebo telefonního odposlechu, až po využití počítačových virů a hackerů. A právě s příchodem a rozšířením internetu je bezpečnost informací sdílených přes tuto celosvětovou síť jednou z nejdůležitějších aktivit všech velkých podniků, ale i domácností a jedinců. S rostoucím počtem uživatelů internetu se zvyšuje také potřeba mít svá data nějakým způsobem chráněná proti zneužití útočníkem, respektive zvyšuje se potřeba zabezpečit informace, které uživatel zadává například při přihlašování ke svému bankovnímu účtu, elektronickému obchodování, ale i třeba „jen“ na fórum některé webové stránky. Nabízí se tedy otázka, jak této bezpečnosti dosáhnout. Ochrana dat je bezesporu spojována s kryptologií, ujasníme si tedy, co se pod tímto pojmem skrývá a podíváme se jak do historie, tak na současné metody, jak eventuálnímu útočníkovi co nejvíce znepříjemnit jeho dobrodružnou práci při snaze získat důležité informace bez našeho svolení.

Bezpečnost na internetu je, jak je psáno výše, velmi úzce spjata s kryptologií, ale drtivá většina podvodů, které se na internetu uskuteční, pramení z chyb, které udělají samotní uživatelé svou vlastní hloupostí. Ano, počítačová negramotnost některých lidí je opravdu zážející. Základem je, jak píše i /1/, nedávat si stejné heslo jako své uživatelské jméno, své heslo nikomu nesdělovat, pokud možno heslo pravidelně obměňovat, používat hesla dostatečně dlouhá, a volit spíše slova, která v běžném slovníku nenajdete.

5.2 Co je to kryptologie

Nejprve by bylo vhodné si ujasnit, co to vlastně ono vznešeně znějící slovo „kryptologie“ znamená. Podle knihy Josefa Zelenky a dalších autorů /24/ je kryptologie (anglicky „cryptology“) samostatná vědní disciplína, která se dělí na kryptografii a kryptoanalýzu, a někdy se také uvádí, že obsahuje steganografii (skrývání zpráv). Kryptografie (anglicky „cryptography“) se zabývá převedením informací do podoby, v níž je obsah této informace před neautorizovanými osobami

skryt, snaží se tedy, aby se zpráva stala pro nepovolané osoby nečitelnou. Tím se liší kryptografie od steganografie, která se zabývá skrýváním zpráv, které ovšem mohou zůstat ve srozumitelné podobě. Dříve měla kryptografie jediný cíl, a to rozvoj algoritmů používaných pro skrytí obsahu zpráv před těmi, kteří nemají povolení je číst. Dnes se už zabývá i rozvojem algoritmů sloužících k jednoznačné identifikaci osoby odesílatele zprávy a k ověření správnosti zprávy (tzv. integrity). Kryptoanalýza (anglicky „cryptoanalysis“) je jakýmsi opakem kryptografie, snaží se ze zašifrované zprávy dostat její původní podobu, snaží se prolomit šifrovací algoritmus.

Mezi další důležité pojmy, které by bylo dobré si vysvětlit na začátku této práce, patří podle Zelenky /24/ kryptografické protokoly a kryptografický systém. Kryptografické protokoly jsou postupem, jak provést šifrování nejvhodnějším způsobem. Základním východiskem pro ně je kryptografický systém, který se stará o transformaci otevřeného textu (plain text) na text šifrovaný (ciphertext).

S použitím internetové encyklopedie /21/ bychom se zde ještě mohli zmínit o dvou pojmech. Slovem šifra, nebo šifrování, budeme nazývat algoritmus, který převádí čitelnou zprávu (prostý text) na nečitelnou zprávu (šifrový text). Klíč je pak tajná informace, bez níž nelze šifrový text přečíst, tzn. nelze provést zpětnou transformaci šifrovaného textu na otevřený.

Šifrovací algoritmy se dají třídit do různých skupin, níže je uvedeno několik vybraných typologií.

➤ Typologie podle množství současně šifrovaného textu:

- bloková šifra – šifruje se určitá skupina symbolů, blok znaků, bývá obvykle pomalejší než druhý typ, proudová šifra
- proudová šifra – z otevřeného na šifrovaný text se převádí znak po znaku, symbol po symbolu

➤ Typologie podle míry utajení kryptografických klíčů:

- klíč musí být utajen – hovoříme o tzv. kryptografii s tajným klíčem
- klíč pro šifrování se může zveřejnit, ale klíč pro dešifrování zůstává tajný – v tomto případě pak mluvíme o kryptografii s veřejným klíčem

- Typologie podle počtu kryptografických klíčů:
 - používá se jeden klíč pro šifrování i dešifrování – kryptografie symetrická
 - pro šifrování a dešifrování různé klíče – kryptografie asymetrická
- Typologie podle možnosti rekonstruovat původní otevřený text:
 - šifrování – otevřený text je možno získat ze zašifrovaného buď se znalostí použitého kryptosystému a klíče, anebo po kryptoanalytickém útoku
 - hašování – původní otevřený text již nelze zpět získat

5.3 Historie Kryptologie

5.3.1 Starověk

Počáteční pokusy o utajení obsahu nějakých zpráv v Egyptě byly pro chápání dnešního člověka opravdu jednoduché, ať už šlo o úpravu klínového písma nebo přidávání znaků známých pouze určité skupině osob.

V Řecku se pak objevuje steganografie (zprávy „ukrývali“ na oholené hlavy poslů, které vyslali se zprávou až poté, co jim dorostly vlasy).

Vedle transpozice, což je promíchání otevřeného textu, se objevují i kódovací tabulky (písmena sepsat do tabulky s očíslovanými řádky i sloupci, každé písmeno pak má svou vlastní souřadnici – za průkopníka tohoto systému je považován řecký spisovatel Polybius). Ze starověku je také známá šifra, které se říká Césarova. Šlo o to, že každé písmeno ve zprávě bylo nahrazeno písmenem o 3 pozice v abecedě dále. Příklady transpozice, kódovací tabulky a Césarovy šifry jsou znázorněny na obrázcích 5.1, 5.2 a 5.3.

Prostý text:
JEDNODUCHY PRIKLAD SIFRY

přepíšeme prostý text do skupin znaků, zápis skupin pod sebe do řádků, následně
píšeme znaky po sloupcích

JEDNO	Šifrovaný text: JDPAR EURDY DCISX NHKIX OYLFX
DUCHY	
PRIKL	
ADSIF	
RYXXX	

Obrázek 5.1 - Transpozice

	1	2	3	4	5	Prostý text: JEDNODUCHY PRIKLAD SIFRY	
1	A	B	C	D	E		Šifrovaný text: 25 15 14 34 35 14 51 13 23 55 41 43 24 31 32 11 14 44 24 21 43 55
2	F	G	H	I	J		
3	K	L	M	N	O		
4	P	G	R	S	T		
5	U	V	W	X	Y		
6	Z						

Obrázek 5.2 - Kódovací tabulky

původní abeceda: ABCDEFGHIJKLMNOPQRSTUVWXYZ
posun o 3 znaky doprava: DEFGHIJKLMNOPQRSTUVWXYZABC

Prostý text:
JEDNODUCHY PRIKLAD SIFRY

Šifrovaný text:
MHGQRFKBSUNOGVLIUB

Obrázek 5.3 - Césarova šifra

5.3.2 Středověk

První významnější evropskou knihu o šifrování sepsal kolem roku 1500 benediktinský opat Trittheim, který se zabýval převážně substitucí, kdy se do textu vloží náhodné znaky, jež mají ztížit případný útok.

V druhé polovině 16. století pak Francouz Blaise de Vigenère představil bezpečnou šifru, jejíž síla spočívala podle /8/ v tom, že k zašifrování zprávy nepoužívá jednu, ale hned několik z 26 odlišných abeced, které spolu nemusejí mít žádnou souvislost a jsou jednoduše definovány posloupností znaků - klíčem, který může mít například i podobu kódového slova. Tím je tato šifra odolná proti klasické frekvenční analýze (což je, jak píše /24/, útok proti monoalfabetickým šifrám spočívající v porovnání frekvence výskytu znaků otevřeného a šifrovaného textu v dané abecedě). Jednoduchý příklad Vigenérovy šifry je na obrázku 5.4.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Obrázek 5.4 - Vigenérova šifra

5.3.3 Dvacáté století

Rozvoj kryptologie doprovází rozvoj techniky, nejznámějším šifrovacím strojem je Enigma. Podle Marka Lloyda /5/ tento německý mechanický šifrovací vynález měnil zprávy před odvysíláním morseovkou do nesrozumitelné směsice. Britské snahy o získání tajemství Enigmy byly úspěšné a výrazně tak ovlivnily průběh druhé světové války.

Ovšem druhá světová válka nebyla jediným válečným nebo politickým konfliktem, ve kterém se ukázala důležitost kryptologie. Jak připomíná Josef Zelenka /24/, v době studené války byla kryptologie chápána jako tajná zbraň a informace o ní byly záměrně potlačovány. Stejně tak Friedmanovo rozluštění japonského „purpurového kódu“ znamenalo pro USA nepřekonatelnou výhodu, která znamenala zničení hlavní úderní síly Japonska (letadlové lodi) u ostrova Midway.

5.3.4 Současnost

V 70. letech se objevil první systém založený na kryptografii s veřejným klíčem, označuje se RSA a používá se dodnes. Ve stejném období byl vyvinut na svou dobu relativně bezpečný symetrický kryptosystém DES. V 90. letech se naskytla možnost pomocí asymetrické kryptografie elektronicky podepisovat dokumenty, teorie se stala praxí a roku 1999 se toto přijalo (formou zákona) i v České republice. Zatímco dříve byla kryptografie výsadou tajných služeb, dnes se stává věcí veřejnou a předmětem výnosného obchodování.

5.4 Steganografie

Na rozdíl od kryptografie, jak se můžeme dočíst v /24/, využívá steganografie ukrývání tajné zprávy do běžné zprávy, do (na) přepravovaných předmětů nebo osob a skrytých komunikačních kanálů. Mezi její nástroje lze zařadit tajný inkoust, odchylky v psaných znacích, jemné vpichy, mřížky pro výběr písmen, vložení zprávy do zasílaného obrázku, textu, audio nahrávky nebo videosekvence apod. Dnes se do souvislosti se steganografií dostávají i vodoznaky, uvádí /13/. Vodoznaky jsou většinou utajené informace podobného charakteru jako steganograficky skrytá zpráva, které slouží jako nezvratný důkaz o autorství.

5.5 Symetrická kryptografie

Symetrická kryptografie používá jeden klíč, který je tajný, a slouží jak k zašifrování zprávy na straně odesílatele, tak i k dešifrování na straně příjemce (zde mohou nastat problémy – důležitá je správa klíčů, udržování klíčů v tajnosti a jejich bezpečná výměna mezi komunikujícími stranami). Výhodou symetrických šifer je nenáročnost na výpočetní techniku, i když záleží na délce zvoleného klíče, a například, jak pro zajímavost uvádí /24/, pro 128 bitový klíč při využití 1000 počítačů by dešifrování trvalo $3,1 \cdot 10^{22}$ let, což je podstatně déle než předpokládaná doba existence našeho vesmíru ($13 \cdot 10^9$ let).

U většiny symetrických šifer je zpracován text po blocích (tzv. bloková šifra), a to o délce 64 bitů, jen například šifra AES používá 128 bitů. Na následujících řádcích jsou uvedeny některé z používaných symetrických šifer.

DES. Data Encryption Standard. Původně tento algoritmus vyvinula firma IBM pod názvem Lucifer. Využívá bloky o délce 64 bitů, ale pro šifrování používá klíč dlouhý jen 56 bitů (8 bitů slouží pro zabezpečení klíče), proto je už dnes tato šifra považována za nedostatečně bezpečnou. Dokonce /17/ uvádí, že při útoku hrubou silou je dnes už možné tuto šifru prolomit do 24 hodin. V důsledku prolomení vznikla zesílená varianta, tzv. 3DES (Tripple DES).

3DES (Tripple DES). Tajemství této šifry spočívá ve vícenásobné aplikaci šifry DES, dvojnásobně, nebo spíše trojnásobně. Pracuje tedy s klíčem o délce 112, respektive 168 bitů.

IDEA. International Data Encryption Algorithm. Jedná se o bezpečný a rychlý algoritmus používající klíč o délce 128 bitů a několik kol výpočtu. Byla používána v PGP (Pretty Good Privacy – počítačový program, který umožňuje šifrování a podepisování). Původně vznikl jako náhrada za DES, vyvíjen byl ve Švýcarsku, dnes je patentován v několika evropských i mimoevropských zemích.

GOST. Zajímavostí tohoto algoritmu je, jak nám stručně shrnuje pan Zelenka /24/, že šifra GOST využívá klíč o délce 256 bitů, a provádí 32 šifrovacích kol výpočtu. Díky tomu je odolná vůči útoku hrubou silou, současně však prodlužuje dobu šifrování.

AES (RIJNDAEL). Advanced Encryption Standard. Podle /16/ byla tato bloková šifra vyvinuta americkou vládou jako standart pro šifrování svých dokumentů. Je to šifra o proměnlivé délce klíče, používá se 128, 192 nebo 256 bitů. Jak uvádí /24/, odolává zatím tato šifra velmi úspěšně všem typům kryptoanalytických úroků (i když je dle mého názoru jen otázkou času, kdy bude prolomena). Je to šifra vhodná pro mnoho typů technického vybavení, zejména pro 8-bitové a 32-bitové procesory. Tuto šifru je také možné použít pro konstrukci hašovací funkce.

SKIPJACK. Pro zajímavost ještě uvádím algoritmus, který byl vyvinut společností NSA (National Security Agency) původně pouze pro obyvatele USA, kde se používal za přísných podmínek, nakonec se však dočkal svého zveřejnění. Používá 80-bitový klíč a 32 kol výpočtu. Tajný klíč se implementoval do čipu typu Clipper, klíč byl rozdělen na dvě části a každá uložena u státem vybrané organizace.

5.6 *Asymetrická kryptografie*

Oproti symetrické používá asymetrická kryptografie dvojici klíčů, kterou si, dle /24/, vygeneruje uživatel pomocí některého z běžně dostupných programů a stává se tak jejich jediným majitelem. Pokud nejde prakticky (s použitím dostupných prostředků) odvodit jeden klíč z druhého, je asymetrická kryptografie označována jako kryptografie s veřejným klíčem. Data zašifrovaná jedním klíčem lze v „rozumném“ čase dešifrovat pouze se znalostí druhého z dvojice klíčů. První klíč (soukromý) je bezpečně ukrýván majitelem, druhý klíč (veřejný) je věrohodně (nejčastěji prostřednictvím certifikační autority) zveřejněn nebo přidělen.

Existují dva základní způsoby použití dvojice klíčů. Prvním způsobem je na odesílanou zprávu použit soukromý klíč odesílatele, dešifrování se provádí pomocí veřejného klíče odesílatele a tím se dá zjistit, že zprávu odeslal právě ten, jehož veřejným klíčem byla zpráva dešifrována, je to jakýsi podpis zprávy. Druhým způsobem je použít na odesílanou zprávu veřejný klíč adresáta, dešifrování pak provádí adresát svým soukromým klíčem a zprávu tak nemůže přečíst nikdo jiný. Tento druhý způsob využívají zejména bezpečnostní protokoly, jako například SSL

(Secure Socket Layer). Oba dva způsoby je však možné kombinovat pro komplexní systém pro utajení i podepsání zprávy.

Jiří Adámek /2/ dále připomíná, že metoda šifrování s veřejně přístupným klíčem je založena na teorii čísel a zejména dvou jejích rysech: existuje rychlý algoritmus k nalezení náhodného prvočísla a neexistuje (respektive není dosud znám) rychlý algoritmus rozkladu velkého čísla v součin prvočísel. Ve své podstatě to znamená, že veřejný klíč je generován s použitím velkých prvočísel a celá bezpečnost (například algoritmu RSA) je založena na problému faktorizace velkých čísel na prvočísla. Základem je výběr dvou velkých (myšleno řádově stovky cifer) prvočísel, která se vynásobí. Na základě jejich součinu je vygenerován jak veřejný, tak privátní klíč. Bez znalosti původních prvočísel je prakticky nemožné součin rozložit zpět na počáteční prvočísla.

Nevýhodou kryptosystémů s veřejným klíčem je jejich pomalost – uvádí se, že asymetrické šifry jsou obvykle 1000krát pomalejší než šifry symetrické (například RSA, o kterém bude řeč dále, je v hardwarové implementaci dokonce 1000krát pomalejší než DES, v softwarové implementaci pak asi 100krát pomalejší /24/). Pár příkladů asymetrických šifer je uvedeno níže.

RSA. Název tvoří iniciály autorů Rivest, Shamir a Aldeman, kteří tento nejoblíbenější algoritmus pro asymetrické šifrování vyvinuli už v roce 1977. Internetová encyklopedie /23/ říká, že je to první algoritmus, který je vhodný jak pro podepisování, tak šifrování. Bezpečnost RSA je postavena na předpokladu, že rozložit číslo na součin prvočísel (faktorizace) je velmi obtížná úloha. Z čísla $n = p \cdot q$ je tedy v rozumném čase prakticky nemožné zjistit činitele p a q . Zcela běžně je dnes RSA použit například pro elektronický podpis, nebo v bankomatech a mobilních telefonech. Používá se s různou délkou klíčů, například 1024 bitů, a podle posledních informací se zatím nikomu nepodařilo tento algoritmus zlomit a je považován na dostatečně bezpečný.

DSA. Digital Signature Algorithm. Podle Josefa Zelenky /24/ používaný ve standardu americké vlády pro digitální podpisy DSS (Digital Signature Standard). Ohledně jeho bezpečnosti jsou neustálé pochyby, i když se opírá o náročnost řešení úlohy diskrétního logaritmu. Nevýhodou je pomalejší verifikace podpisu než jeho generování.

D-H. Deffie-Hellman je nejstarší algoritmus s veřejným klíčem, ale stále se ještě používá pro výměnu klíčů. Stejně jako DSA se opírá o složitost výpočtu diskrétního logaritmu.

El Gamal. Jedná se o variaci D-H určenou k šifrování. Ovšem podle [18] má nevýhodu takovou, že šifrovaná data jsou dvakrát tak delší než data nešifrovaná. To nejspíš bude důvodem, proč není tak často používán jako RSA.

5.7 Hašovací funkce

Jak říká definice Jiřího Příbyla [7], hašovací funkce je výpočetně efektivní funkce, která transformuje (mapuje) posloupnosti binárních symbolů libovolné délky na binární posloupnosti určité konstantní délky, nazývané hašé hodnoty. Stejně tak se můžeme dočíst ([24], [19]), že se jedná o jednosměrnou funkci, což je taková funkce, z jejíhož výsledku se velmi obtížně odvozuje její předpis (vstup).

Nejčastěji se dnes většina uživatelů internetu setkává s hašovacími funkcemi v případě, kdy se přihlašují na webové stránky a zadávají své heslo. Toto heslo se při registraci uživatele, i následném přihlášení, však neukládá do databáze uživatelů ve své původní podobě, ale už jako hašé hodnota (pokud je hašovací funkce použita – dnes už, dalo by se říci, nutnost).

Celý princip spočívá v tom, že zadané heslo při registraci slouží jako vstup pro hašovací funkci, která toto heslo převede na přesně dlouhý řetězec, a ten se poté uloží do databáze uživatelů ke konkrétnímu přihlašovacímu jménu. Při následném přihlašování, kdy uživatel opět zadává vedle loginu i heslo, je opět heslo převedeno hašovací funkcí na hašé hodnotu, a ta je pak porovnávána s údajem v databázi. Pokud je shoda, uživatel je přihlášen, jinak ne. Tím je zajištěna bezpečnost, jelikož z principu jednosměrné funkce vyplývá, že kdyby se útočníkovi podařilo získat hašé hodnotu uloženou v databázi, nepodaří se mu z této hašé hodnoty zpět získat původní (prostý) text.

Mezi nejznámější hašovací funkce patří MD5, SHA-1 a SHA-2. Dále je uveden stručný popis těchto hašovacích funkcí, následně pak na obrázku 5.5 se můžete

podívat na jednoduchý příklad hašovací funkce MD5 a SHA-1 na slově KRYPTOLIGIE.

MD5. Jak se můžeme dočíst v /22/, MD5 je 128-bitová hašovací funkce, hojně využívána například pro kontrolu integrity souborů nebo ukládání hesel. Ovšem je to už funkce poměrně zastaralá (vznikla roku 1991 jako náhrada dřívější MD4). Dnes už se nepovažuje za dostatečně bezpečnou, proto se doporučuje používat spíš SHA-1 nebo SHA-2.

SHA-1. Secure Hash Algorithm. Vytvoří na rozdíl od MD5 kontrolní haš dlouhý 160 bitů. Je přibližně o čtvrtinu pomalejší než zmíněná MD5, ale za to bezpečnější. Ovšem ani SHA-1 není už zcela bezpečná, protože jak píše /11/, stejně jako MD5 už byl algoritmus SHA-1 prolomen.

SHA-2. Od SHA-1 se odlišuje tím, že má 256 bitový kód. Mělo by se tedy jednat o zatím nejbezpečnější ze zmíněných hašovacích funkcí, ovšem na jak dlouho? Například Přemysl Souček /14/ uvádí, že on sám potřeboval k prolomení MD5, která má 128 bitový kód a dříve byla považována za bezpečnou po mnoho let, pouhých 17 vteřin!

Prostý text: KRYPTOLOGIE Hašé text – po použití MD5: dc27ababb1e09a153e8ae5affa83fc81 Hašé text – po použití SHA-1: 2e997b4bccdf280fbae1e1ad56a0eb365ace4cc1

Obrázek 5.5 - Hašovací funkce

6 Náhled na možný budoucí stav přístupu k informacím

6.1 Počítačová gramotnost

V dnešním moderním světě, kdy ve vyspělých zemích je počítač téměř v každé domácnosti, by už výuka práce na počítači a s internetem měla být samozřejmostí. Už na základních školách se s tímto učením začíná a je to jediné dobře. Stále více informací se ukládá právě do elektronické podoby, a proto je nezbytné, aby je lidé byli schopni vyhledávat a používat.

Zatímco dříve se žáci a studenti s počítačem nesetkali téměř vůbec a pokud se chtěli něco o nich naučit, pracovat s nimi, museli hledat odborné a placené kurzy. Proto dnes ve starší populaci nenajdeme mnoho takových, kteří by měli s počítačem bohaté zkušenosti. Dokonce i mezi mladší generací se najde nemalá část lidí, kteří jsou rádi, že vědí jak počítač zapnout a vypnout, napsat e-mail, přečíst si textový dokument a to je všechno. Samozřejmě, mohou se specializovat na určitý obor nebo pracovní pozici, ve které počítač nepotřebují. Ale přiznejme si, svět se vyvíjí a hlavně přizpůsobuje se vývoji informačních a komunikačních technologií.

Rozhodně je přínosné, že výuka práce s počítači probíhá na základních, středních i vysokých školách. Se zvyšující se kvalifikací by lidé měli být i lépe schopni počítač a internet ovládat a vědět, jak nejlépe je využít při zaměstnání a vyhledávání a zpracovávání informací. Zajímavé by bylo, kdyby se na středních školách tato výuka ještě více rozšířila. Tak jako na odborných středních školách a učilištích se maturita skládá nejen ze 4 předmětů, ale i z pátého praktického předmětu. Proč tedy nezavést praktický předmět i na gymnáziích? A nejen tam, i na obchodních, ekonomických nebo průmyslových školách je mnoho nadaných studentů, kteří se chystají se studiem po maturitě nepřestávat a získat nějaký vysokoškolský diplom. Myslím, že povinná maturita z informatiky by určitě nebyla na škodu, ba naopak.

Jen díky větší podpoře učení s počítači a internetem mohou vzniknout nové individuality, které budou u zrodu dalších technických pokroků. Pokud si už na

základní či střední škole počítač natolik oblíbí, aby se jeho struktuře nebo práci s ním věnovali i ve volném čase a rozvíjeli si své schopnosti, může z nich vyrůst elita počítačové gramotnosti a mohou to být právě oni, kteří se zapíší zlatým písmem do dějin svými novými objevy v rámci informačních a komunikačních technologií.

6.2 Představa vývoje přístupu k informacím

Je logické, že se změnou v technických vymoženostech, se mění i možnosti, jak informace ukládat, vyhledávat, zpracovávat. Stejně tak jako po vzniku knihtisku se šířily knihy neskutečnou rychlostí, se vznikem počítačů se rozšiřují elektronické informace. Tento trend bude pokračovat i v budoucnosti, stále více a více dokumentů bude v počítačových systémech.

Knihovny se také změnily, s novými médii přibily i služby, které nabízejí. Jak to bude dále? Nezanikne náhodou tištěná literatura pod obrovským množstvím elektronických dat? Rozhodně ne. I dnes je pro mnoho a mnoho lidí příjemnější učit se a číst si knihy a časopisy v klasické podobě. Knihy nezmizí, dále budou existovat i knihovny. Ale malá změna by jim určitě slušela.

Například by se mohly rozšířit možnosti knihoven, nemuseli by nabízet jen klasické knihy a časopisy, ale třeba i důležité a placené informace v elektronické podobě. Staly by se z nich instituce s obrovským přínosem pro člověka. Čtenář by navštívil z domova internetové stránky knihovny, vybral si požadovanou informaci a díky informačnímu systému by mohl za obdrženou informaci zaplatit například pomocí svého bankovního účtu, jednoduchým převodem. Samozřejmě by se musela vyřešit otázka bezpečnosti, ale už dnes existuje mnoho internetových obchodů, kde je možnost platit pomocí platební karty a účtu v bance. Podobný systém by se tedy dal využít i při placení za služby spojené se získáváním důležitých informací.

Internet a celkově komunikační sítě budou v budoucnu hrát ještě větší roli ve všech směrech. Jak v zábavě, tak v obchodu a podnikání. Spojit se s přáteli na druhé straně planety a i vidět, co právě dělají, už nepředstavuje nějaký větší problém. Stejně tak telefonické porady a videokonference jsou již dnes běžně používány v prosperujících a rozsáhlých firmách, určitě je v tom velký potenciál i do budoucna.

Pro mnoho lidí by odpadly problémy spojené s dopravou do práce, když by mohli své záležitosti řešit z domova a s kolegy, nadřízenými i podřízenými se spojit prostřednictvím internetu. Leckdy by tak bylo rychlejší sdělit si informace tímto způsobem, než osobně dojít do kanceláře na druhém konci chodby.

Obecně práce s informacemi se nevztahuje jen na to, co nám může pomoci v podnikání, nebo na to, abychom věděli, jakou si vybrat novou postel. Hodně často sdělujeme naše osobní informace, při podepisování smluv, pokud jsme nemocní, nebo i když nás v autě zastaví policejní hlídka. Proč lidem trochu neulehčit peněženky? Vše by se zjednodušilo, pokud by se začaly používat jednotné elektronické průkazy, zároveň občanský a řidičský průkaz, průkaz pojištěnce, a další a další v jednom malém s naskenovanou fotografií, jako to známe ze studentských karet. Informace o nás bychom tak měli v jedné přehledné kartičce. Podrobné informace by pak byly k dispozici při přiložení tohoto průkazu k čtecímu zařízení, tak by si okamžitě mohli pracovníci banky ověřit, jestli nemáme nějaké nesplacené půjčky, policisté pak třeba, zda už jsme se někdy dopustili dopravního přestupku a jak závažného. Zjednodušila by se tím práce mnoha lidem, dost věcí by se urychlilo.

Informační a komunikační technologie obrovskou měrou přispěly k automatizaci a rychlosti získávání a sdělování informací po celém světě. I v příštích letech a desetiletích přinesou lidem velký prospěch, ať už ve formě finančního zisku, nebo většího času na své blízké. Vždy ale bude záležet na tom, co budou lidé schopni a ochotni akceptovat, jaké technologické vymoženosti používat, a jaké ne. Lidský faktor odjakživa byl, je a bude, tedy alespoň doufám, tím rozhodujícím. Vždy záleží na člověku, jakou použije metodu při hledání řešení, jestli zapne počítač nebo ne, kde se rozhodne informace hledat a jak je pak zpracuje. Informační a komunikační technologie mu v jeho práci jen pomáhají a usnadňují ji.

7 Závěr

Pojem informace je v posledních letech a desetiletích stále více zmiňován. Ať si pod ním představíme obsah toho, co je komunikováno mezi dvěma lidmi, nebo nějaké důvěrné údaje o konkurenční firmě, jsou informace důležité. Informace neboli význam, který přiřazujeme datům, však lidé chápou jinak, rozdílně. Dva jiní lidé proto mohou na základě stejných údajů vykonat různá rozhodnutí. Je to dáno osobnostním fondem každého jedince, který se tvoří od našeho narození celou dobu našeho života a je ovlivňován tím, jak jsme vychováni, v jakých sociálních poměrech vyrůstáme, jaké na nás působí kulturní prostředí. To vše je důvodem, proč jsou lidé jiní, i když byli všichni vybaveni od přírody nejdůležitějším orgánem nervové soustavy, mozkiem. Proto se můžeme v mnoha významných firmách při pracovních pohovorech na důležité místo setkat s různými testy, které by měli personálním pracovníkům této organizace pomoci ve výběru toho nejlepšího na danou pozici.

Pro každého člověka jsou správné informace základem efektivního rozhodování. Ovšem musí to být opravdu informace správné, protože mnohokrát se setkáváme s informacemi, které rozhodně správné nejsou. Může se stát, že budou zastaralé, nebo mohou být špatně zpracovány, v nejhorším případě mohou být úmyslně chybné. Opravdu, pokud použijeme informace, které jsou naprosto chybné, mohou nás takové informace stát velmi mnoho, daleko víc než cena, kterou jsme za tyto informace zaplatili. Firmy mohou přijít o svou dobrou pověst, o zákazníky, obyčejní lidé pak třeba i o své zdraví. Pokud si ale získané informace dokážeme ověřit, potvrdit či vyvrátit jejich správnost, takovéto riziko snížíme. Měli bychom se tedy snažit o čerpání informací z více zdrojů, a nechat si je potvrdit. Dobrým postupem může být i zkoumání chybných rozhodnutí z minulosti, neboť stále platí, že z chyb se člověk učí. Můžeme se totiž dostat do podobné situace, jako někdo před námi, a budeme vědět, jakou cestou se rozhodně nevydat, abychom neudělali také chybu. Pokud se tímto vším budeme řídit, pak jediné můžeme navrhnout řešení určitého problému takové, abychom ho mohli považovat za optimální.

Všechny informace ale musíme někde získat, najít. Nejsnadnější způsob je, pokud je máme ve své vlastní paměti, ale ne vždy se na vlastní paměť můžeme spolehnout, proto zde opět platí potřeba si informace ověřit ještě z jiného zdroje. Kromě našich známých a expertů můžeme využít celou škálu takovýchto zdrojů. Mezi nejvýznamnější patří určitě knihovny, které obsahují mnoho a mnoho zajímavých a užitečných publikací. S příchodem počítačů a internetu se postupně více a více informací sděluje právě elektronickou cestou. Internet sám o sobě v sobě skrývá velký potenciál, co se týká práce s informacemi, tedy jak jejími vyhledáváním, získáváním i šířením. Ale přiznejme si, že kromě těchto skvělých možností v sobě nese i velkou hrozbu. Hrozbu takovou, že se informace dostanou do nepovolaných rukou. Může se jednat o citlivé informace, které si přečte malé dítě, pak je tu nebezpečí, že se podle nich bude řídit. Druhým problémem může být odcizení důvěrných informací například k využití v konkurenčním boji. Leckdy je metoda nelegálního získání cenných informací, například o výrobním procesu úspěšného produktu, velkým lákadlem. Je to rychlejší a i levnější než se pokusit vlastními výzkumy docílit podobné úspěšnosti. Proto se mnoho vědců a odborníků zabývá nejrůznějšími metodami, jak si svá data co nejlépe chránit.

Mít své informace bezpečně uložené je doslova nezbytné. K ochraně dat zejména, ale nejen, na internetu je důležité vědět, co je to kryptologie. Právě ta se zabývá kódováním zpráv, které se mají dostat jen k tomu, komu jsou určeny. Stejně tak se věnuje rozluštění již zakódovaných zpráv. I v kryptologii vidíme jasné změny s ohledem na vývoj informačních a komunikačních technologií. Od jednoduchých prastarých metod, jako například Césarova šifra, nebo kódovací tabulky, se přešlo k novějším. Přes miniaturní fotoaparáty využívanými v průmyslové špionáži, až po moderní šifrovací algoritmy či hašovací funkce, které převedou různě dlouhý řetězec znaků na jiný pevně dlouhý řetězec, který nejde zpět rekonstruovat na původní text. Proto jsou tyto hašovací funkce a jejich neustálé zdokonalování tak nezbytné pro větší zabezpečení našich informací na internetu. Stále se zrychlují počítačové procesy, lidé přicházejí s novými nápady, a leckteré metody chránění informací, dříve považované za bezpečné, jsou dnes zcela nedostačující.

Právě i s tímto, aby se dále pracovalo na zdokonalování zabezpečovacích algoritmů, souvisí nutnost vysoké počítačové gramotnosti. Záleží tak jen na nás, jestli budeme chtít počítačům více rozumět, nebo je jen používat.

8 Seznam použitých zdrojů

- /1/ ABSOLUT BEGINNER ON WWW. *Volba hesla a jeho utajení před světem* [online]. [citováno 2007-04-09]. URL: < <http://www.abowe.brbla.net/1-kapitola-uzivatelske-minimum/bezpecnost-zaklady/volba-hesla-utajeni.php> >.
- /2/ ADÁMEK, Jiří. *Kódování*. 1. vydání. Praha – SNTL Nakladatelství technické literatury, 1989. 192 stran.
- /3/ BRÁZA, Jiří. *Internet.cz: Jak hledat a najít*. 3. vydání. Praha - vydavatelství Grada Publishing s.r.o., 2001. 128 stran. ISBN 80-247-9002-5.
- /4/ CEJPEK, Jiří. *Informace, komunikace a myšlení (uvod do informační vědy)*. 1. vydání. Praha - Karolinum - nakladatelství Univerzity Karlovy, 1998. 179 stran. ISBN 80-7184-767-4.
- /5/ LLOYD, Mark. *Guinnessova kniha špionáže*. 1. vydání. Praha – nakladatelství Olympia, 1996. 255 stran. ISBN 80-7033-413-4.
- /6/ NAGEL, Kurt. *Úspěch! Strategie a metody*. 5. vydání. Praha - vydavatelství Grada a.s., 1992. 232 stran. ISBN 80-85454-50-9.
- /7/ PŘIBYL, Jiří. *Informační bezpečnost a utajování zpráv*. 1. vydání. Praha – České vysoké učení technické, 2004. 239 stran. ISBN 80-01-02863-1.
- /8/ SECURITY-PORTAL.cz. *Praktické základy Kryptologie a Steganografie* [online]. [citováno 2007-04-09]. URL: < <http://www.security-portal.cz/clanky/prakticke-zaklady-kryptologie-a-steganografie.html> >.
- /9/ SKYFLIERS. *Hong Kong International Airport*. [online]. [citováno 2007-05-02]. URL: < <http://www.skyfliers.com/hongkong2.php> >.
- /10/ SKYFLIERS. *Letiště Hong Kong, Kai Tak*. [online]. [citováno 2007-05-02]. URL: < <http://www.skyfliers.com/hongkong.php> >.
- /11/ SLASHDOT. *SHA-1 Broken* [online]. [citováno 2007-04-09]. URL: < <http://it.slashdot.org/it/05/02/16/0146218.shtml?tid=93&tid=172&tid=218> >.
- /12/ SMETÁČEK, Vladimír. *Informace o informacích*. Praha - vydavatelství

- Grada a.s., 1993. 152 stran. ISBN 80-85623-22-6.
- /13/ SPECIALISTA.INFO. *Steganografie* [online]. [citováno 2007-04-09]. URL:
< <http://www.specialista.info/view.php?cislocclanku=2005090125> >.
- /14/ SVĚTVĚCÍ.CZ. *Elektronický podpis už neznamená jistotu* [online]. [citováno 2007-04-09]. URL:
< <http://aktualne.centrum.cz/technika/svet-pocitacu/clanek.phtml?id=282000> >.
- /15/ TENZER, Oliver - PSTRUŽINA, Karel. *Svět moderního myšlení*. 1. vydání. Praha - Nakladatelství Svoboda, 1984. 260 stran.
- /16/ WIKIPEDIA. *Advanced Encryption Standard* [online]. [citováno 2007-04-09]. URL:
< http://cs.wikipedia.org/wiki/Advanced_Encryption_Standard >.
- /17/ WIKIPEDIA. *Data Encryption Standard* [online]. [citováno 2007-04-09]. URL: < http://cs.wikipedia.org/wiki/Data_Encryption_Standard >.
- /18/ WIKIPEDIA. *ElGamal* [online]. [citováno 2007-04-09]. URL:
< <http://cs.wikipedia.org/wiki/ElGamal> >.
- /19/ WIKIPEDIA. *Hašovací funkce* [online]. [citováno 2007-04-09]. URL:
< http://cs.wikipedia.org/wiki/Ha%C5%A1ovac%C3%AD_funkce >.
- /20/ WIKIPEDIA. *Informace*. [online]. [citováno 2007-04-29]. URL:
< <http://cs.wikipedia.org/wiki/Informace> >.
- /21/ WIKIPEDIA. *Kryptografie* [online]. [citováno 2007-04-08]. URL:
< <http://cs.wikipedia.org/wiki/Kryptografie> >.
- /22/ WIKIPEDIA. *MD5* [online]. [citováno 2007-04-09]. URL:
< <http://cs.wikipedia.org/wiki/MD5> >
- /23/ WIKIPEDIA. *RSA* [online]. [citováno 2007-04-09]. URL:
< <http://cs.wikipedia.org/wiki/RSA> >.
- /24/ ZELENKA, Josef – ČAPEK, Jan – FRANCEK, Jiří – JANÁKOVÁ, Hana. *Ochrana dat. Kryptologie*. 1. vydání. Hradec Králové – nakladatelství GAUDEAMUS Univerzity Hradec Králové, 2003. 198 stran. ISBN 80-7041-737-4.

9 Seznam obrázků

<i>Obrázek 2.1 - Shannonova teorie informace - komunikační kanál</i>	11
<i>Obrázek 2.2 - Vývoj neuronových struktur (převzato z /15/)</i>	14
<i>Obrázek 5.1 - Transpozice</i>	38
<i>Obrázek 5.2 - Kódovací tabulky</i>	38
<i>Obrázek 5.3 - Césarova šifra</i>	38
<i>Obrázek 5.4 - Vigenérova šifra</i>	39
<i>Obrázek 5.5 - Hašovací funkce</i>	45

KNIHOVNA VŠE

ZÁZNAM O BAKALÁŘSKÉ PRÁCI

AUTOR	Jan Láznička	
NÁZEV BP	Měnicí se význam a vliv informací	
FAKULTA	Fakulta informatiky a statistiky	
OBOR	Informatika	
ROK OBHAJOBY	2007	
POČET STRAN	53	
POČET PŘÍLOH	0	
VEDOUCÍ BP	Ing. Antonín Rosický, CSc.	
ANOTACE	Jedinečnost lidského myšlení a osobnostní fond každého člověka. Význam a vliv informací na lidské rozhodování. Odkud informace získávat, srovnání dřívějších metod a dnešních nepoužívanějších zdrojů. Bezpečnost informací.	
KLÍČOVÁ SLOVA	informace, informatika, rozhodování, zdroje informací, bezpečnost	
	MÍSTO ULOŽENÍ	SIGNATURA