

## Material do egzaminu z modułu I.

Informacje zawarte w niniejszym materiale zostały opracowane na podstawie treści zawartych w:

- Słownik komputerowy: <http://sloownikkomputerowy.pl/>,
- Wikipedia – wolna encyklopedia: <http://pl.wikipedia.org/>,
- Podręcznik: Informatyka. Podstawowe tematy. Nowe wydanie. Autor: Grażyna Koba. Rok wydania: 2009,
- Czasopisma: PC Format, PC World, Chip,
- Syllabus\_5.pdf i inne źródła.

### Material zawarty w podręczniku do informatyki od strony 8 do strony 25.

(proszę powtórzyć przed egzaminem)

1. **Hardware** – sprzęt komputerowy, wszystkie jego podzespoły (mechaniczne, elektryczne i elektroniczne) oraz urządzenia zewnętrzne, takie jak: drukarka, skaner, mysz, klawiatura itd. Hardware działa dzięki zainstalowanemu w nim oprogramowaniu (ang. software).
2. **Porty wejścia/wyjścia** komputera to gniazda, za pośrednictwem których są przyłączane do komputera urządzenia zewnętrzne. Wyróżnić można: porty wejściowe do podłączenia klawiatury i myszy, porty wyjściowe do podłączenia monitora i drukarki oraz porty wejścia - wyjścia do przyłączenia komputera do sieci.
3. **Port szeregowy** (ang. *Serial Port*) – port komputerowy, przez który dane są przekazywane w formie jednego ciągu bitów. Port ten jest zwykle zaopatrzony w specjalny układ o nazwie UART, który tłumaczy ciągi bitów na bajty i na odwrót.  
Komputery klasy PC mają zwykle kilka portów szeregowych – jeden lub dwa porty RS-232, dwa złącza PS/2 i kilka portów USB. Komputery przenośne są także często wyposażone w port podczerwieni. Porty szeregowy w komputerze wykorzystuje się zwykle do podłączania "strumieniowych" urządzeń zewnętrznych takich jak myszy, klawiatury, modemy, urządzenia pomiarowe. Ze względu na prostszą synchronizację niż w przypadku portu równoległego, porty szeregowy w praktyce osiągają większe przepustowości. Teoretyczna przepustowość portów równoległych jest większa, ponieważ nie istnieje ograniczenie ilości równoległe wykorzystywanych linii sygnałowych.  
Port szeregowy jest często błędnie utożsamiany z magistralą RS-232 ponieważ port COM początkowo był najpopularniejszym portem szeregowym wyprowadzonym na zewnątrz komputera PC.
4. **Port równoległy** (ang. *Parallel Port*) – port w technice komputerowej, w którym dane są przesyłane jednocześnie kilkoma przewodami, z których każdy przenosi jeden bit informacji. Przeciwnieństwem portu równoległego jest port szeregowy.  
W komputerach klasy PC używa się kilku portów równoległych. Najbardziej znanym jest port o standardzie Centronics (LPT) przesyłający jednocześnie 8 bitów danych, został on zaprojektowany do przesyłania danych między komputerem a drukarką. Innymi portami równoległymi są SCSI i ATA.  
Jako że port Centronics jest najczęściej jedynym portem równoległym wyprowadzonym na zewnątrz komputera klasy PC, port równoległy jest z nim błędnie utożsamiany.
5. **Czytnik ekranowy** (ang. *screen reader*) to program komputerowy, który rozpoznaje i interpretuje informacje wyświetlane na monitorze komputera, a następnie przedstawia je użytkownikowi w postaci głosowej lub zostaje wysłany do brajlowskiego urządzenia wyjściowego. Czytniki ekranowe są formą technologii asystujących, wykorzystywaną m.in. przez osoby niewidome i niedowidzące, lub

prowadzące samochody czy obsługujące szereg komputerów jednocześnie.

Wiele systemów operacyjnych zawiera wbudowane screen readersy takie jak Narrator (MS Windows), VoiceOver (Apple Inc Mac OS X) i in. Najczęściej używanymi czytnikami ekranu są ciągle produkty komercyjne jak np. Jaws, czy Window-eyes, ale szybki rozwój programów open source, takich jak NVDA dla Windows i GNOME dla Linux powodują, że zdobywają one coraz większą popularność oferując możliwości analogiczne do oprogramowania komercyjnego.

6. **Upload** (ang.) - w informatyce, proces przeciwny do downloadu, polegający na wysyłaniu plików lub innych danych do serwera lub komputera należącego do innego użytkownika.

Często łącze internetowe jest umownie dzielone na dwa kanały: upload i download. Przepustowość tych kanałów (czyli ich prędkość) mierzy się w kilobitach na sekundę (kbps). Łącza internetowe popularne w warunkach domowych (ADSL, telewizja kablowa, sieć osiedlowa itp.) ze względu na ich stosunkowo niewysoką cenę, są często asymetryczne, czyli mają zaniżoną przepustowość kanału "Upload" umożliwiającego wysyłanie danych w stosunku do kanału "Download", umożliwiającego odbieranie danych. Z tego powodu upload pliku jest znacznie wolniejszy niż download.

7. **FireWire** to standard łącza szeregowego umożliwiającego szybką komunikację i synchroniczne usługi w czasie rzeczywistym. Opracowany w roku 1995 dla komputerów osobistych i cyfrowych urządzeń optycznych. Rozwijany przez firmę Apple Inc. Jest zdefiniowany w dokumencie IEEE 1394.

Magistrala ta w okrojonej wersji (brak linii zasilających) wykorzystywana jest przez firmę Sony (a obecnie również inne) pod nazwą **i.Link**. Natomiast firma Creative Technology opisuje złącze jako SB1394. Zmiana nazwy ma na celu uniknięcie opłat licencyjnych, ale wszystkie te złącza są ze sobą w 100% zgodne.

FireWire jest szeregową magistralą ogólnego przeznaczenia, jednak ze względu na promowanie jej przez Apple jako wyjątkowo multimedialnej oraz ze względu na powszechne stosowanie w kamerach jest kojarzona prawie wyłącznie z kamerami cyfrowymi. Obecnie popularne stało się używanie FireWire w profesjonalnych kartach muzycznych i innym sprzęcie audio.

8. **Forum dyskusyjne (internetowe)** to przeniesiona do struktury stron WWW forma grup dyskusyjnych, która służy do wymiany informacji i poglądów między osobami o podobnych zainteresowaniach przy użyciu przeglądarki internetowej.

Fora dyskusyjne są obecnie bardzo popularną formą grup dyskusyjnych w Internecie. Prowadzą je praktycznie wszystkie portale, większość wortalii, znaczna liczba ISP. Są one także powszechne na stronach wielu instytucji, czasopism, przedsiębiorstw, uczelni itp. a także spotykane są liczne fora zakładane zupełnie prywatnie.

9. **Czynniki zwalniające pracę komputera:**

- a. Fragmentacja dysku twardego. Z czasem użytkowania komputera dysk twardy ulega fragmentacji. Jest to zjawisko polegające na pojawianiu się nieciągłości obszarów zapisanych i niezapisanych. Najpoważniejszym skutkiem fragmentacji systemu plików jest spadek wydajności operacji na plikach. Duża fragmentacja zmusza do częstej kalibracji głowicy dysku twardego.
- b. Wirusy, robaki oraz groźne pliki, które zwalniają prace komputera.
- c. Niedobór pamięci RAM (512 MB). Do bardziej komfortowej zabawy w nowych grach dołożenie kolejnej kości 512MB jest wręcz przymusem.
- d. Uruchomienie jednocześnie wielu programów np. graficznych, gier itp. na tym samym komputerze.

10. **Pamięć RAM** - (ang. Random Access Memory). Pamięć wewnętrzna komputera o dostępie bezpośrednim (swobodnym), w której czas dostępu do dowolnego jej elementu jest taki sam. Jest to

pamięć ulotna, czyli jej zawartość znika po wyłączeniu zasilania komputera. Przechowywany w niej jest wykonywany program (lub jego część) i przetwarzane przez program dane. Kolejne wersje oprogramowania korzystają z coraz większej pamięci RAM. (512 MB, 1 GB – 1024 MB, 2 GB).

11. **ROM** (ang. Read-Only Memory - pamięć tylko do odczytu) - rodzaj pamięci urządzenia elektronicznego, w szczególności komputera. Zawiera ona stałe dane potrzebne w pracy urządzenia - np. procedury startowe komputera, czy próbki przebiegu w cyfrowym generatorze funkcyjnym. Z pamięci tej dane można tylko odczytywać. Są w niej przechowywane podstawowe dane, które muszą zostać zachowane nawet jeśli urządzenie nie jest zasilane.
12. **Pamięć masowa - pamięć zewnętrzna**, zwana również pamięcią pomocniczą, jest nieulotna. Przechowywane są w niej programy i dane, które nie są wykorzystywane w danej chwili. Warto wiedzieć, jaką pojemność mają obecnie różne rodzaje pamięci w komputerach IBM PC:
  - dysk twardy – 40 GB, 80, 160 GB, 500 GB, 1TB;
  - dyskietka - 1.44 MB;
  - płyta CD-ROM - 650 MB, 700 MB;
  - płyta DVD - 4,6 GB, 9,2 GB;
  - taśma strimera - 20 MB, 40 MB.
  - pamięć USB (znana także pod nazwami: PenDrive, USB Flash Drive, Flash Disk, FlashDrive, Finger Disk, Massive Storage Device, Flash Memory Stick Pen Drive, USB-Stick) - urządzenie przenośne zawierające pamięć nieulotną typu Flash EEPROM, zaprojektowane do współpracy z każdym komputerem poprzez port USB i używane do przenoszenia danych (zapisywanych w plikach) między komputerami. Najczęściej występujące pojemności to: 128 MB, 256 MB, 512 MB, 1 GB, 2 GB, 4 GB, 8 GB, 16GB, 32GB, 64GB, 128GB. Opracowano również urządzenia o pojemności 256 GB.
  - Blu-ray Disc (BD) – konkurencyjny dla HD DVD format zapisu optycznego, opracowany przez Blu-ray Disc Association (BDA). Następca formatu DVD. Wyróżnia się większą pojemnością od płyt DVD, co jest możliwe dzięki zastosowaniu niebieskiego lasera. Ten nowy typ nośnika pozwala na zapisanie 25 GB danych na płytach jednowarstwowych. W użytku są również płyty dwuwarstwowe o pojemności 50 GB.
13. **Urządzenia wejścia** – urządzenia zewnętrzne komputera służące do wprowadzania danych. Zalicza się do nich: klawiaturę, mysz, wszelkiego rodzaju czytniki pisma (znaków) i innych kodów (np. kodu paskowego), a także skaner. Powstają urządzenia, które w przyszłości będą służyły człowiekowi do komunikacji z komputerem za pomocą głosu. W pewnym sensie sieć Internet jest również urządzeniem wejściowym, gdyż można z niej pobierać dane i informacje do przetwarzania.
14. **Urządzenia wyjścia** – urządzenie zewnętrzne komputera służące do wyprowadzania wyników jego pracy. Zalicza się do nich: ekran monitora, drukarkę. Wyniki są często zapisywane w pamięci zewnętrznej, np. na dysku lub płycie CD. W pewnym sensie sieć Internet jest również urządzeniem wyjściowym, gdyż można w niej umieszczać i udostępniać wyniki pracy na komputerze, np. w postaci stron WWW.
15. **Software – oprogramowanie**. Zespół programów tworzących pewną zamkniętą całość i przeznaczony do ściśle określonych zadań. Na przykład oprogramowanie edukacyjne to programy edukacyjne wspomagające i wzbogacające nauczanie; oprogramowanie użytkowe składa się z programów użytkowych, przeznaczonych do posługiwania się nim w wybranej dziedzinie zastosowań (zalicza się do nich m.in. edytory tekstu, edytory grafiki, arkusze, bazy danych); oprogramowanie DTP służy do komputerowego składu, czyli przygotowania publikacji do druku; oprogramowanie narzędziowe tworzą w komputerze programy narzędziowe, które są przeznaczone do wykonywania czynności zarządzających plikami itd.

16. **System operacyjny** – program, który sprawuje pełną kontrolę nad działaniem komputera i pełni funkcję pośrednika między użytkownikiem a systemem komputerowym. Uruchamiany jest po włączeniu komputera i działa aż do jego wyłączenia. Do zadań systemu operacyjnego, częściowo zleczanych mu przez użytkownika, należy m.in.: wykonywanie operacji na plikach (np. kopiowanie, przenoszenie), zapewnienie komunikacji między wszystkimi elementami i urządzeniami komputera, kontrola urządzeń wejścia/wyjścia, uruchamianie programów. Znane systemy operacyjne: MS-DOS, Windows (wersje 3.11, 95, 98, XP, 2000, Win 7) i Linux dla komputerów IBM PC oraz Unix dla większych komputerów. W obecnie produkowanych systemach operacyjnych jest wykorzystywany graficzny interfejs użytkownika.
17. **Zadania wykonywane przez podstawowe rodzaje software to:**
- oprogramowanie edukacyjne to programy edukacyjne wspomagające i wzbogacające nauczanie;
  - oprogramowanie użytkowe składa się z programów użytkowych, przeznaczonych do posługiwania się nim w wybranej dziedzinie zastosowań (zalicza się do nich m.in. edytory tekstu, edytory grafiki, arkusze, bazy danych);
  - oprogramowanie DTP służy do komputerowego składu, czyli przygotowania publikacji do druku;
  - oprogramowanie narzędziowe tworzą w komputerze programy narzędziowe, które są przeznaczone do wykonywania czynności zarządzających plikami itd.
18. **Profil użytkownika** – dane wprowadzone za pomocą strony „o sobie”. Poprzez treść upublicznią rozumie się treść wprowadzoną przez zalogowanego użytkownika serwisu udostępnianą za pomocą serwisu innym użytkownikom sieci. Jako treść upublicznią rozumie się w szczególności: profil użytkownika, opis miejsca, opis wydarzenia.
19. **Sieć LAN** – sieć lokalna, lokalna sieć komputerowa (ang. *Local Area Network*)  
Sieć utworzona z komputerów znajdujących się w niewielkiej odległości od siebie. Na ogół taka sieć jest budowana w jednej instytucji, np. w szkole i służy lokalnym potrzebom komunikacyjnym tej instytucji. Sieć lokalna jest często połączona z siecią Internet, co umożliwia każdemu użytkownikowi komputera w sieci lokalnej dostęp do sieci Internet. Dzięki niewielkim odległościom między komputerami, sieci lokalne charakteryzują się dużymi prędkościami przesyłania danych. Najpopularniejszym systemem operacyjnym sieci lokalnej jest Netware firmy Novell oraz sieciowe środowisko firmy Microsoft, np. system Windows Server 2003, bardzo często występujące w szkolnych sieciach komputerowych. Sieci lokalne są łączone ze sobą w sieć miejską, a dalej – w sieć rozległą.
20. **Sieć WAN** (z ang. Wide Area Network, rozległa sieć komputerowa) – sieć komputerowa znajdująca się na obszarze wykraczającym poza jedno miasto (bądź kompleks miejski).
21. **Podcasting, podcast, spolszczone: podkasting, podkast** to forma internetowej publikacji dźwiękowej lub filmowej, najczęściej w postaci regularnych odcinków, z zastosowaniem technologii RSS. (np. [www.podcast.pl/](http://www.podcast.pl/))  
Nazwa wzięła się z połączenia słów iPod - odtwarzacz muzyczny firmy Apple i broadcast (z ang. transmisja, przekaz). Początki podkastingu sięgają roku 2000. Wówczas to pojawił się pierwszy szkic dotyczący użycia technologii RSS do publikowania treści audio i wideo. Gwałtowny wzrost zainteresowania podkastingiem nastąpił na przełomie lat 2004 i 2005. O ile jeszcze pod koniec września 2004 liczba wyników zwracanych przez wyszukiwarkę Google oscylowała w granicach 500, to rok później było to ponad sto milionów. Google Trends datuje pierwsze zapytania odnośnie słowa podcast na koniec września 2004.  
Aby słuchać podkastów nie trzeba posiadać iPod'a ani innego odtwarzacza muzycznego - wystarczy komputer odtwarzający cyfrowe pliki dźwiękowe (np. w formacie MP3) lub pliki wideo w przypadku podkastu wideo oraz oprogramowanie pobierające i katalogujące transmisje na podstawie informacji

zawartych w publikowanych razem z podkastami plikach RSS. Wiele podkastów nie wymaga nawet tego, publikując bezpośrednio linki do plików na stronach WWW.

Podkast może mieć formę nieformalnego bloga, profesjonalnej audycji radiowej, kursu językowego lub hobbystycznego albo odcinków historii czytanej przez lektora. Istnieje coraz więcej powieści, które pierwszych odbiorców znalazły jako odcinki publikowane w postaci podkastów (Earthcore, Ancestor i "Infection" Scotta Singlera, Deja Vu Iana Hocklinga, Tom Corven Paula Story), a inne są rozpowszechniane jako podkast, aby zwiększyć popularność wersji drukowanej i ułatwić publikację kolejnych części ("Brave Men Run" Matthew Wayne Selznicka). Prezydent USA George W. Bush publikował swoje sobotnie przemówienia w formie podkastów. Wielkie korporacje medialne takie jak CNN oraz BBC wprowadziły w ramach testów swoje podkasty. Ich śladem poszło również Polskie Radio. Uczelnie Berkeley i Stanford udostępniają w formie podkastów wybrane wykłady, muzykę i audycje radia studenckiego.

## 22. Globalna sieć komputerowa – Internet

Ogólnoświatowa sieć komputerowa. Złożona jest z mniejszych sieci, rozlokowanych w różnych instytucjach edukacyjnych (szkoły, wyższe uczelnie), przemysłowych, administracyjnych i rządowych. Komunikacja między różnymi sieciami i komputerami w różnych sieciach jest możliwa dzięki zastosowaniu i przyjęciu przez wszystkie sieci tego samego protokołu TCP/IP, który służy do wymiany pakietów z danymi między komputerami użytkowników i serwerami.

Internet łączy wszystkie ważniejsze instytucje na świecie. W tej sieci zostały już zgromadzone olbrzymie zasoby informacji w postaci: tekstów, obrazów, dźwięków i filmów oraz ich multimedialnych aranżacji.

Internet zapewnia wiele usług związanych z dostępem do zgromadzonych w niej informacji oraz wymianą informacji i komunikacją.

Do najważniejszych należą:

– Dostęp do zgromadzonych zasobów informacji i możliwość udostępniania swoich zasobów na stronach WWW.

– Wymiana informacji i komunikacja za pośrednictwem: poczty elektronicznej, list i grup dyskusyjnych, pogawędek.

– Dostęp do zasobów w postaci programów (FTP).

Tak rozległy i powszechny dostęp do informacji stwarza jednak zagrożenie dla praw twórców i autorów oraz dla własności intelektualnej.

Historia sieci Internet rozpoczęła się w latach sześćdziesiątych w Stanach Zjednoczonych w atmosferze zimnej wojny, gdy zastanawiano się, jak zapewnić komunikację między najważniejszymi punktami w państwie na wypadek wojny. Prototypem sieci Internet była sieć ARPANET, zbudowana w 1967 roku. W Polsce pierwsze połączenie ze światową siecią uzyskano w 1990 roku przez Kopenhagę.

## 23. Szybkość transferu danych.

**Bit na sekundę** (ang. *bps – bit per second*) – jednostka natężenia strumienia danych w medium transmisyjnym (np. pomiędzy dwoma komputerami) oraz jednostka przepustowości, czyli maksymalnej ilości informacji, jaka może być przesyłana przez dany kanał telekomunikacyjny w jednostce czasu, oznaczana **b/s** bądź **bps**.

Powszechnie stosuje się wielokrotności bitu na sekundę. Mogą być one wyrażane z użyciem przedrostków dziesiętnych SI (**kilobit na sekundę**, **megabit na sekundę**) albo przedrostków binarnych IEC 60027–2 (**kibibit na sekundę**, **mebibit na sekundę**).

**kb/s, kilobit na sekundę** (ang. *kilobit per second*)

Nie należy mylić z **kilobajtami na sekundę**. Skrócony zapis tych dwóch jednostek jest niemal identyczny, różni się jedynie wielkością litery 'B'. **Kilobity na sekundę** to kb/s (małe 'b'), natomiast **kilobajty na sekundę** to kB/s (wielkie 'B'). Ta subtelna różnica w zapisie nie jest adekwatna do różnicy między tymi jednostkami w rzeczywistości, ponieważ 1 kb/s to szybkość transmisji dokładnie 8 razy mniejsza niż 1 kB/s (1 kB = 8 kb).

Jednostkę *kilobity na sekundę* stosuje się powszechnie do określania maksymalnej przepustowości kanału komunikacji (np. łącza internetowego). Nie służy jednak do określania prędkości przesyłu danych w danym momencie, wielkość taką opisujemy za pomocą *kilobajtów na sekundę*.

**Mb/s (Mbit/s), megabit na sekundę**

1 Mb/s =  $10^6$  b/s = 1 000 000 b/s.

**Gb/s, gigabit na sekundę**

1 Gb/s =  $10^9$  b/s = 1 000 000 000 b/s.

#### 24. Sposoby łączenia się z Internetem.

Do najpopularniejszych sposobów dostępu do Internetu w naszym kraju należą:

– łącza stałe o przepustowości od 64 kb do 2048 kbit/s – są to tak zwane łącza ADSL i DSL. Są one najczęściej oferowane przez TP SA (Neostrada) i charakterystycznym dla nich jest to, iż każdy klient posiada zewnętrzny numer IP. W naszym kraju są także dostępne łącza o transferze około 100 Mbit/s jednak ich koszt jest bardzo wysoki i ich zastosowanie ma miejsce tylko dla wielkich przedsiębiorstw takich jak np. portale internetowe,

– łącza modemowe (Dial-up) o przepustowości około 56 kbit/s. Łącze analogowe, w obecnych sytuacjach jest ono niewystarczające dla większości potrzeb, jednak dalej pozostaje podstawowym sposobem łączenia się z Internetem. Było bardzo popularne podczas początków rozwoju Internetu w naszym kraju. Następstwem zwykłego modemu stały się urządzenia oparte o technologię ISDN pracujące na linii cyfrowej.

– łączenie się z Internetem przy pomocy sieci lokalnej jest bardzo popularnym sposobem, który na pewno wzbogaca zwykle łącza stałe. Zwykle serwer sieci LAN posiada łącze stałe (np. typu DSL), które to jest udostępnione dla innych komputerów w sieci. Taki sposób dostępu do Internetu to jeden z najprostszych i najbezpieczniejszych. Oprócz tego użytkownicy sieci mogą bardzo szybko wymieniać ze sobą dane, czego nie ma przy innych sposobach dostępu do Internetu. Coraz popularniejsze stają się także sieci LAN oparte na technologii radiowej, WLAN, gdzie stosuje się radiową komunikację w zakresie 2,4 GHz i 5,4 GHz. Do istniejącej struktury sieci LAN dokłada się dodatkowo kilka punktów dostępowych, przez co obszar, który obejmuje dana sieć rozszerza się do nawet kilku kilometrów. Jest to także możliwość dotarcia do tych użytkowników, którzy znajdują się zbyt daleko od sieci LAN i nie ma możliwości doprowadzenia do nich kabla koncentrycznego.

- łącze telewizji kablowej. Z dostępnych w Polsce ofert właśnie ta najbliższa jest znaczeniu magicznego angielskiego słowa "broadband" - czyli dostęp szerokopasmowy. Co prawda nominalna przepustowość internetowej sieci kablowej równa się osiągom Neostrady, jednak lepsze połączenia z innymi sieciami sprawiają, że z reguły można z niej "wycisnąć" znacznie więcej. Kabłówka to rozwiązanie, które można z (w miarę) czystym sumieniem polecić amatorom internetowego radia, gier sieciowych, transmisji wideo i internetowych rozmów telefonicznych.

#### 25. Połączenia szerokopasmowe.

Szerokopasmowy dostęp do Internetu (z ang. Broadband) to usługa polegająca na połączeniu z Internetem za pomocą szybkiego łącza o dużej przepustowości transmisji danych. Najczęściej do tego celu wykorzystuje się technologię DSL, xDSL, ISDN, 3G, WiMAX/WiFi, a także technologie sieci telewizji kablowej i łącza światłowodowe.

Dostęp szerokopasmowy umożliwia transmisję danych z dużą prędkością, co najmniej 1 - 2 Mb/s do odbiorcy (download) i 512 kb/s od odbiorcy (upload). Jednak aby korzystać w pełni z możliwości multimedialnych Internetu, konieczne jest symetryczne łącza o prędkości ponad 20 Mbit/s pozwalające na oglądanie filmów HD w czasie rzeczywistym.

- Firmy telekomunikacyjne w technologii ADSL – szerokopasmowy dostępu do Internetu za pomocą tej samej infrastruktury, z której korzysta telefon stacjonarny, w Polsce zwykle 1 - 2 Mb/s, a maksymalnie do 8 - 10 Mb/s.
- Telewizje kablowe - szerokopasmowy dostęp oferowany przez większość telewizji kablowych przy wykorzystaniu infrastruktury płatnej telewizji kablowej. Prędkość łącza: 512 kb/s – 1 Mb/s.

26. **Technologie informacyjno - komunikacyjne (ICT)** – wszelkie działania związane z produkcją i wykorzystaniem urządzeń telekomunikacyjnych i informatycznych oraz usług im towarzyszących, a także gromadzenie, przetwarzanie, udostępnianie informacji w formie elektronicznej z wykorzystaniem technik cyfrowych i wszelkich narzędzi komunikacji elektronicznej.

27. **Komunikator internetowy (ang. Instant Messenger, od tego skrót IM)** – program komputerowy pozwalający na przesyłanie natychmiastowych komunikatów (komunikacja natychmiastowa – ang. Instant Messaging) pomiędzy dwoma lub więcej komputerami, poprzez sieć komputerową, zazwyczaj Internet (dlatego komunikatory internetowe). Od poczty elektronicznej różni się tym, że oprócz samej wiadomości, przesyłane są także informacje o obecności użytkowników, co zwiększa znacznie szansę na prowadzenie bezpośredniej konwersacji.

Komunikatory przesyłają informacje według zasad ustalonych przez protokoły komunikacyjne tak, że publicznie udokumentowane protokoły są zwykle implementowane przez wiele komunikatorów, zapewniając prawie nieograniczone grono odbiorców, podczas gdy protokoły utajnione zmuszają użytkowników do korzystania z programów przygotowanych przez producentów, ograniczając tym samym możliwość komunikacji.

Komunikatory bardzo często łączą użytkowników przez serwery, do których przyłączają się, i od których działania są uzależnione. Niekiedy tak skrajnie, że użytkownik skazany jest na reklamy emitowane przez producenta aplikacji.

Oprócz programów obsługujących tylko jedną sieć IM, powstały także multikomunikatory, które umożliwiają komunikację z użytkownikami różnych sieci poprzez zestaw wtyczek. Popularne programy tego typu to Tlen, Konnekt, Miranda IM, AQQ, Pidgin, Kopete, czy Trillian. W sieci Jabber komunikacja z innymi sieciami zapewniana jest przez serwer poprzez system transportów.

Użytkownicy w sieciach IM posiadają jednoznaczne identyfikatory, które pozwalają na precyzyjne określenie odbiorcy komunikatów. Część sieci (np. ICQ, Gadu-Gadu) przydziela swoim użytkownikom identyfikatory liczbowe, zazwyczaj metodą "pierwszy wolny". Inne, np. Tlen, MSN czy Yahoo umożliwiają wybranie własnej nazwy. Szczególnym rozszerzeniem tego sposobu jest identyfikowanie użytkowników w sieci Jabber/XMPP. Jako że nie ma w nim centralnego serwera, niezbędne jest określenie w identyfikatorze nazwy serwera na którym zarejestrowany jest użytkownik – identyfikatory w Jabberze przypominają adresy poczty elektronicznej (np. `uzytkownik@example.com`).

Zagrożenia wynikające z użytkowania komunikatorów.

Poprzez komunikatory, tak jak i pocztę elektroniczną bardzo popularne stało się rozsyłanie tzw. SPIM-u (odpowiednika SPAM-u występującego w poczcie elektronicznej) w przykładowej postaci łańcuszków internetowych, podejrzanych linków, które niejednokrotnie zawierają wirusy. Kolejną wadą i zagrożeniem jest fakt, iż takie rozmowy mogą być przechwytywane, podsłuchiwane, gdyż komunikatory internetowe są najczęściej darmowe, często więc producent nie przywiązuje większej wagi do ich bezpieczeństwa. Możliwy jest więc brak odpowiedniego szyfrowania przesyłanych komunikatów (treść rozmowy przesyłana czystym tekstem) oraz haseł do konta. Ale największym chyba zagrożeniem jest tzw. cyber bullying, co oznacza po prostu cyberprzemoc, gdzie zamiarem ludzi ją stosującej - jest wyrządzenie krzywdy psychicznej i poniżenie ofiary.

28. **E-bankowość. W podręczniku do informatyki rozdział 4. Inne usługi Internetowe, str. 116 – 118.**

#### Home banking

Rozwiązanie to umożliwia obsługę rachunków bankowych bez konieczności wychodzenia z domu. Obsługa rachunku bankowego odbywa się przy użyciu publicznej sieci telefonicznej, telefonii komórkowej lub innego łącza dostępowego oraz komputera wyposażonego w odpowiednie oprogramowanie. Bezpieczeństwo systemu zapewniają m.in. generowane hasła, a transmitowane dane są kodowane. Wadą HomeBankingu jest to, że dostęp do konta jest możliwy tylko z komputera, na którym jest zainstalowany program.

### Bankowość internetowa

Komunikacja z bankiem za pośrednictwem Internetu. Witryna internetowa banku umożliwia klientom dokonywanie on-line różnorodnych operacji na ich rachunkach. Klient banku internetowego powinien mieć dostęp do komputera z zainstalowaną przeglądarką stron WWW podłączonego do sieci Internet.

### Phone banking i mobile banking

Usługi bankowe dostępne za pośrednictwem telefonu nazywamy bankowością telefoniczną lub phone bankingiem. Te dostępne dzięki urządzeniom przenośnym, głównie telefonom komórkowym, określamy jako bankowość mobilną lub mobile banking.

Operacje bankowe przez telefon mogą być realizowane na kilka sposobów: poprzez kontakt z operatorem (call center) lub automatyczny serwis telefoniczny IVR oraz przy użyciu telefonu komórkowego za pomocą SMS lub technologii WAP.

Operacje wykonywane za pomocą bankowości telefonicznej możemy podzielić na pasywne i aktywne. Pasywne to takie, gdzie klient odbiera jedynie informacje dotyczące rachunku. Najprostszą i najczęściej wykonywaną operacją pasywną jest sprawdzenie salda rachunku. Inne, dostępne w większości serwisów telefonicznych, usługi to sprawdzanie historii rachunku bądź uzyskiwanie informacji o aktualnych stopach oprocentowania lub kursach walut. Usługi aktywne bankowości telefonicznej to takie, które powodują zmianę salda i historii rachunku. Do typowych operacji aktywnych zaliczyć możemy przelewy oraz dyspozycje dotyczące lokat terminowych.

### Teletekst

Istnieje też możliwość sprawdzenia stanu konta przez teletekst. W Polsce tę usługę proponował wyłącznie Invest Bank. Klient musiał zadzwonić do teleserwisu banku, podać (tonowo) swój numer PESEL oraz hasło. Serwis podawał numer strony teletekstu. Od tej chwili na podanej stronie teletekstu programu Polsat przez 3 minuty były wyświetlane dane konta (saldo i operacje). Tak wyświetlane informacje dostępne były dla wszystkich osób posiadających telewizor z teletekstem. Pomimo iż bank nie wyświetlał nazwy klienta i numeru rachunku, a czas wyświetlania danych konta był stosunkowo krótki to taki sposób prezentacji oznaczał brak poufności danych.

### Email banking

Istnieją dwa rodzaje tej usługi.

Pierwsza z nich ma bierny charakter. Klient posiada na serwerze bankowym skrzynkę poczty elektronicznej. Na koniec każdego dnia bank wysyła na tę skrzynkę informację o dokonanych tego dnia transakcjach i aktualnym stanie konta, chyba że danego dnia nie została wykonana żadna operacja.

Drugą oferowaną formą email banking (aktywną), jest usługa E-mail Money, choć faktycznie jest ona odmianą WWW lub WAP Bankingu. Umożliwia dokonywanie przelewów. Aby skorzystać z tej usługi nie trzeba znać numeru rachunku odbiorcy, wystarczy adres jego poczty elektronicznej. W celu dokonania takiego przelewu na stronie internetowej banku podaje się adres e-mail odbiorcy, kwotę, jaką chce się mu przesłać oraz pytanie i odpowiedź dla celów weryfikacyjnych. Nadawca takiego przekazu dostaje od banku powiadomienie o nim na swoją skrzynkę pocztową. Następnie loguje się na witrynie banku w celu podania odpowiedzi na zadane pytanie, a gdy się wszystko zgadza, podaje numer rachunku bankowego, na który mają być przelane środki pieniężne.

### Karty płatnicze

Za pomocą karty płatniczej klienci mogą dokonywać operacji w bankomatach i wpłatomatach oraz dokonywać transakcji za pośrednictwem terminali POS.

### **Korzyści płynące z bankowości elektronicznej**

#### Dla klienta

- niższe koszty przeprowadzonych operacji - poprzez eliminację zarówno pośrednich jak i bezpośrednich kosztów obsługi klienta, oferowane usługi stały się bardziej atrakcyjne pod względem cenowym.
- zwiększenie satysfakcji - dostępność wirtualnych usług bankowych 24 godziny na dobę, 7 dni w tygodniu daje klientom komfort psychiczny jak i w znacznym stopniu stanowi duże udogodnienie z racji dostępu do usług bankowych z dowolnego miejsca bez konieczności fizycznej obecności w placówce banku.



- bieżący kontroling - bankowość elektroniczna umożliwia swoim klientom sprawowanie bieżącej kontroli nad własnym rachunkiem, sprawdzenie salda, dokonywanie transakcji bezgotówkowych, co jest gwarancją poczucia bezpieczeństwa a także formą nadzoru sytuacji finansowej.
- wygodna komunikacja - bankowość elektroniczna oznacza brak konieczności stania w kolejkach do okienka bankowego (a nawet wychodzenia z domu) szybki i łatwy dostęp do informacji. Wszystko czego potrzebuje klient by mieć dostęp do pełnej informacji to urządzenie elektroniczne (np.: telefon, komputer)

#### Dla banku

- zwiększenie wyników finansowych banku - co w głównej mierze wynika ze zmniejszenia kosztów stałych dla banku lub też rozłożenia ich na większą liczbę użytkowników.
- promowanie szerokiego asortymentu usług i produktów - bankowość elektroniczna jest szybkim kanałem dostępu zarówno do już pozyskanych jak i potencjalnych klientów. Internet, telefon, WAP czy SMS stanowią wygodny sposób do informowania klienta o nowych usługach, aktualnych stopach procentowych czy też kampaniach promocyjnych.
- możliwość zebrania cennych informacji o klientach - operacje dokonywane przez klientów są skrupulatnie analizowane w celu wyselekcjonowania ich segmentów, preferencji i lepszego dostosowania usług do potrzeb klienta.
- indywidualizacja oferty - analiza preferencji klienta pozwala na stworzenie profilu klienta i sporządzenia specjalnej dla niego oferty spełniającej jego oczekiwania i indywidualne preferencje.
- możliwość dotarcia do licznej grupy - elektroniczne kanały dostępu stanowią idealny nośnik informacji zarówno do klienta indywidualnego jak i masowego przejawiającego zainteresowanie usługami bankowymi.

#### Bezpieczeństwo

Jednym z głównych problemów bankowości internetowej są systemy bezpieczeństwa. Systematyczny wzrost wartości transakcji w Internecie uzasadnia konieczność ciągłego doskonalenia systemów bezpieczeństwa. Bezpieczeństwo transakcji ma podstawowe znaczenie w budowaniu zaufania pomiędzy klientem a bankiem. Mimo że obecnie stosowane rozwiązania techniczne zapewniają niezbędny poziom bezpieczeństwa transakcji przeprowadzanych za pomocą Internetu, nadal widoczna jest bariera psychologiczna, która skutecznie wpływa na liczbę instytucji decydujących się na transakcje sieciowe. Ciągła praca nad doskonaleniem zabezpieczeń tych systemów i sukcesy w tej dziedzinie powodują jednak, że usługi oferowane przez banki internetowe stają się równie pewne, jak usługi banków uniwersalnych.

#### Cztery główne metody zapewniające bezpieczeństwo to:

- Szyfrowana transmisja danych - realizowana za pośrednictwem protokołu SSL.
- Proste uwierzytelnianie - (identyfikator, hasło, PIN).
- Silne uwierzytelnianie - (np. token, certyfikat użytkownika, klucz prywatny).
- Podpis elektroniczny.

29. **E-nauczanie – e-learning** - nauczanie z wykorzystaniem technik komputerowych i Internetu, oznacza wspomaganie dydaktyki za pomocą komputerów osobistych, CDROM-u i Internetu. Pozwala na ukończenie kursu, szkolenia, a nawet studiów bez konieczności fizycznej obecności w sali wykładowej. Doskonale uzupełnia również tradycyjny proces nauczania. E-learning to tylko jeden z elementów edukacji, dlatego edukacja w czasie rzeczywistym dotyczy znacznie obszerniejszego zasięgu usług niż e-learning.

Termin e-learning, tak jak i techniki uczenia się oraz technologie kształcenia, odnosi się do stosowania w nauczaniu technologii elektronicznej w o wiele szerszym zakresie niż w ramach tradycyjnych szkoleń komputerowych, czy też nauczania wspomaganego komputerowo z połowy lat osiemdziesiątych. Jest również o wiele szerszy od pojęć nauczania i edukacji online, które oznaczają nauczanie tylko przez sieć internetową. W przypadku zastosowania technologii mobilnych, częściej używane jest pojęcie M-learningu.

E-learning służy nauczaniu na odległość oraz nauczaniu elastycznemu, jednak może być również

łączony z tradycyjnym nauczaniem w formie kursów mieszanych. Ponadto e-learning umożliwia nam samodzielne wybranie preferowanego formatu dostarczania wiedzy i tempa jej przekazywania.

Dostęp do zautomatyzowanych narzędzi oraz materiałów dydaktycznych umożliwia typowe środowisko e-learningowe Virtual Learning Environment (VLE) z menu nawigacyjnym i ikonami.

Szczególnie w szkolnictwie wyższym wzrasta tendencja do tworzenia środowisk VLE, które w połączeniu z systemami kontroli informacji (Managed Information System, MIS), tworzą system kontroli środowiska e-learningowego (Managed Learning Environment). W środowiskach tych wszelkie informacje związane z kursem przekazywane są poprzez interfejs użytkownika zgodny ze standardami obowiązującymi na uczelni.

Coraz więcej tradycyjnych szkół wyższych, jak również młodszych szkół wyższych online, oferuje przez Internet wybrane programy dyplomowe na wielu poziomach i w wielu dziedzinach. Zazwyczaj studenci zobowiązani są do uczęszczania na zajęcia, jednak wiele kursów jest udostępnianych wyłącznie online. Ponadto, coraz częściej uczelnie oferują studentom wsparcie online np. w formie informacji i rejestracji w sieci, e-doradztwa, sprzedaży podręczników przez Internet, stron samorządów czy gazet studenckich online.

E-learning może również odnosić się do edukacyjnych stron internetowych, udostępniających np. scenariusze lekcji, arkusze ćwiczeniowe, czy interaktywne ćwiczenia dla dzieci. Pojęcie to jest również używane w biznesie w odniesieniu do odpłatnych szkoleń online.

#### Wady i zalety

Do zalet e-learningu często zalicza się ruchomy czas pracy i wygodę uczniów (szczególnie jeśli mają oni jeszcze inne zobowiązania), ułatwienie komunikacji między uczniami, lepsze dostosowanie do potrzeb uczniów, większe urozmaicenie nauki dzięki zastosowaniu multimediów i niewerbalnej prezentacji materiału. E-learning pozwala uczyć się we własnym tempie oraz zminimalizować strach i nieśmiałość, które mogłyby pojawić się w tradycyjnej klasie. Użycie technik wideo umożliwia uczenie się za pomocą materiału audiowizualnego, który można zatrzymać i przewinąć w celu ponownego obejrzenia. W porównaniu z tradycyjnymi zajęciami w klasie, e-learning przynosi duże zyski organizacjom z rozproszonymi i ciągle zmieniającymi się uczniami (np. personel restauracji). Niektórzy krytykują zastosowanie e-learningu w edukacji, ponieważ brak w nim osobistego kontaktu z nauczycielem i w związku z tym, jak twierdzą niektórzy, nie jest on już „edukacyjny” w ujęciu czysto filozoficznym (np. wg definicji R.S. Petersa, filozofa edukacji). Zwolennicy e-learningu twierdzą, że ta krytyka jest w dużej mierze bezpodstawną, ponieważ relacje międzyludzkie można rozwijać przy zastosowaniu programów audio lub wideo służących do prowadzenia konferencji internetowych, forów dyskusyjnych, czatów, blogów, poczty elektronicznej, lub innych synchronicznych czy asynchronicznych środków. Właściwie wielu uczniów amerykańskich szkół średnich byłoby za zajęciami w formie e-learningu gdyby nie jego bardziej skrajne wersje, zmierzające ku wyeliminowaniu osobistego kontaktu z nauczycielem.

Często mówi się też o wrażeniu odosobnienia, którego doświadczają uczniowie uczący się na odległość, chociaż fora dyskusyjne i inne formy komunikacji komputerowej mogą zmniejszyć to wrażenie, a nawet zachęcać do kontaktów osobistych i tworzenia grup wzajemnej pomocy. W sieci mogą również powstawać grupy dyskusyjne. Należy wspierać kontakty międzyludzkie w każdej formie, zarówno między wykładowcą a uczniem jak i między uczniami.

Odpłacalność e-learningu jest przedmiotem szerszej dyskusji ponieważ zazwyczaj większość wkładu początkowego zwraca się dzięki efektowi skali (economies of scale). Koszt rozwoju sieci, a w szczególności zwykłego oprogramowania może być taki sam jak koszt systemów dostosowywanych specjalnie do e-learningu. Opracowanie materiałów kompatybilnych z e-learningiem jest również bardziej czasochłonny niż opracowanie tych zwykłych.

W rezultacie część kosztów muszą ponieść studenci ponieważ kursy online w szkołach wyższych są zazwyczaj droższe od tych tradycyjnych.

Zaletą szczególnie w działalności firm jest oszczędność pieniędzy - eliminacja kosztów związanych z prowadzeniem szkoleń w sposób tradycyjny, tym samym znikają z budżetu takie pozycje jak: honorarium trenera, wynajem ośrodka szkoleniowego, transport, zakwaterowanie, wyżywienie i inne. Ponadto można wspomnieć o braku dezorganizacji pracy. Tradycyjne szkolenia, w których

uczestniczy większa część grupy (działu) znacznie utrudniają i dezorganizują pracę, co często negatywnie odbija się na efektach pracy lub powoduje straty. Kolejną zaletą jest duża oszczędność czasu. Szkolący się pracownicy nie tracą czasu na dojazdy do miejsca szkolenia i nie muszą odrywać się od swoich codziennych zajęć. Poza tym przełożeni mogą nadzorować efekty szkolenia i postępy w nauce swoich pracowników.

30. **Telepraca (zdalna praca), biuro w domu**, forma organizacji pracy polegająca na świadczeniu pracy poza siedzibą przedsiębiorstwa, jednak w kontakcie z przełożonymi i współpracownikami za pomocą urządzeń telekomunikacyjnych.

Te urządzenia to: telefon, telefaks, wideofon. Dzięki coraz powszechniejszej dostępności światowej sieci informatycznej - Internetu w telepracy zastosowanie znalazła poczta elektroniczna (*e-mail*), oraz stała się możliwa praca grupowa i praca przez Internet, dzięki zdalnemu dostępowi do zasobów sieci komputerowej przedsiębiorstwa. O wyborze odpowiedniej techniki decyduje specyfika wykonywanej pracy.

Cel: poprawa produktywności i redukcja kosztów (dojazdy, powierzchnia biurowa).

Wymagania: sprawnie działająca sieć telekomunikacyjna.

Uważa się, że telepraca umożliwia pracownikom łatwiejsze pogodzenie obowiązków służbowych ze sprawami osobistymi i rodzinnymi. Jest to zaletą szczególnie dla kobiet karmiących piersią. Telepraca to również możliwość zatrudnienia osób niepełnosprawnych.

W praktyce nie jest to takie oczywiste.

Jeśli sytuacja nie jest przymusowa, kobiety i niepełnosprawni chcą wyrwać się ze środowiska, w którym czują się jak uwięzieni. Zajmowanie się dzieckiem lub osobą niepełnosprawną nie pozostawia czasu na pracę pełnoetatową; pozostaje przyjmowanie zleceń. Menedżerowie też muszą posiadać umiejętności precyzyjnego planowania i koordynowania pracy: zdalne nadzorowanie, instruowanie, uzgadnianie poglądów - są trudne, a czasem niemożliwe.

Przykłady telepracowników:

- administratorzy sieci,
- tłumacze,
- księgowi,
- dziennikarze,
- pracownicy naukowci,
- przedstawiciele handlowi.

Zalety telepracy to przede wszystkim:

- redukcja kosztów wynajmu pomieszczeń biurowych, dojazdów do pracy, a także kosztów zatrudnienia,
- wzrost wydajności pracy,
- elastyczność miejsca i czasu pracy dla pracownika,
- możliwość zatrudniania osób niepełnosprawnych i korzystających z urlopu wychowawczego,
- zmniejsza konflikty w pracy.

Wady telepracy:

- trudność w odseparowaniu pracy od domu,
- brak bezpośredniego nadzoru / kontroli,
- dłuższy dzień w pracy,
- uzależnia od techniki - technologie w wersjach jednostanowiskowych są w dzisiejszych czasach bardziej awaryjne i relatywnie droższe w naprawie niż zapewnienie serwisu dla firmy wielostanowiskowej,
- osłabia osobiste kontakty między pracownikami.

31. **Komunikacja tekstowa**

Nie jest tajemnicą, że komunikacja tekstowa jest bardzo powszechna wśród nastolatków nie tylko u nas. Aktualnie dominuje wysyłanie SMS-ów, ale już niebawem dostaną oni nowe możliwości dzięki taniemu Internetowi mobilnemu i zaawansowanym technologicznie *smartphone*'om.

W Australijskim Monash University przeprowadzono badania na próbie dzieci w wieku od 11 do 14 lat, które są użytkownikami telefonów. Badano jakość komunikacji. Okazuje się, że przez nadmierną komunikację dzieci mogą być ogłupiane: wiadomości są krótkie, nie wyrażają emocji, czy rozbudowanych opinii. To fakt: operatorzy uczą nas, że opinię na dany temat musimy zmieścić w 160 znaków, co może zaowocować uproszczeniem schematów myślenia, a emocje są zastępowane emotikonami. Także pojawiają się częste literówki. Ponadto dzieci preferują szybkość komunikacji nad jej jakością, czy to gramatyczną, czy logiczną. Pojawia się wiele skrótów i wyrażen ze slangu internetowego.

32. **Komunikacja w Internecie** – zagrożenia i ostrzeżenia, podręcznik strona 129, rozdział 3.
33. **RSI** (ang. *Repetitive Strain Injury*) - urazy na skutek chronicznego przeciążenia mięśni i ścięgien. Powstają na skutek długotrwałego powtarzania czynności. Często wśród pracowników linii montażowych, piszących na klawiaturze, graczy używających myszy komputerowych, sekretarek i pracowników IT. Choroba ta jest powodowana głównie długotrwałym utrzymywaniem tej samej pozycji ciała - siedzenie bez możliwości przerwy przez długi czas; bądź wykonywaniem powtarzających się czynności - obsługa komputera za pomocą myszy i klawiatury, granie na gitarze, praca narzędziami ręcznymi.
34. **Licencja użytkownika końcowego EULA** (od ang. *End User License Agreement*) - zapis definiujący warunki udzielenia licencji końcowemu użytkownikowi oprogramowania..  
Ważna informacja prawna dla wszystkich użytkowników: przed rozpoczęciem korzystania z oprogramowania należy uważnie przeczytać umowę licencyjną.  
Klikając przycisk wyrażam zgodę na umowie licencyjnej, użytkownik wyraża zgodę na przestrzeganie jej warunków i zasad. Czynność ta jest jednoznaczna ze złożeniem podpisu, a użytkownik wyraża zgodę na przestrzeganie umowy, której staje się stroną oraz wyraża zgodę na egzekwowanie jej postanowień w sposób obowiązujący w przypadku wszelkich wynegocjowanych, pisemnych umów podpisanych przez użytkownika. Jeżeli użytkownik nie wyraża zgody na wszystkie lub niektóre zasady i warunki umowy, powinien przerwać instalację oprogramowania i zrezygnować z instalacji.  
Po kliknięciu przycisku wyrażenia zgody w oknie umowy licencyjnej, użytkownik nabywa prawo do korzystania z oprogramowania na zasadach i warunkach zawartych w umowie.
35. **Co to jest Really Simple Syndication (RSS)** – technika przesyłania nagłówków wiadomości wraz z funkcją powiadamiania o nowościach.  
Informacja na witrynach: <http://serwisy.gazeta.pl/rss/>, <http://www.tvn24.pl/rss.html>, <http://www.rssy.pl/>.
- RSS (popularnie rozwijane jako *Really Simple Syndication*) to alternatywny w stosunku do standardowych stron WWW sposób dostępu do zasobów Internetu, zwłaszcza wiadomości i blogów. Metoda dystrybucji nagłówków wiadomości, oparta na standardzie XML. Zestaw nagłówków umieszczonych w pliku RSS tworzy tak zwany kanał RSS. Do odczytu tego typu wiadomości służą specjalne programy, tak zwane czytniki RSS. Czytniki RSS automatycznie pobierają nowe wiadomości, gdy tylko te zostaną opublikowane. Skrót RSS oryginalnie rozwijało się jako Really Simple Syndication (nie mającego sensownego odpowiednika w języku polskim). Obecnie uznaje się, że RSS to po prostu format internetowych wiadomości zapisanych w plikach XML. RSS przypomina popularne *newslettery*, z tym że wiadomości docierają do prenumeratora indywidualnie i natychmiast po tym, jak zostają opublikowane (a nie np. raz dziennie).
- RSS (Really Simple Syndication) to sposób rozpowszechniania informacji publikowanych na stronach WWW. Wiadomości RSS są dostarczane w formie nagłówków i przypominają pocztę elektroniczną - mają tytuł, skrót i odnośnik, który prowadzi do pełnej informacji na stronie WWW.
- Jakie są zalety RSS-ów?
- Korzystając z RSS-ów możesz zebrać w jednym miejscu informacje z wielu źródeł na

interesujące cię tematy.

- Nie musisz oglądać wielu reklam i ładować ciężkich stron ze zbędnymi informacjami przed dotarciem do tego, co cię interesuje. Dzięki RSS-om omijasz spam!
- Korzystając z RSS-ów nie musisz ściągać na swój komputer nic więcej, niż "spis treści" wybranych serwisów internetowych - dlatego skrót RSS oznaczał oryginalnie *Rich Site Summary* (Rozszerzony Spis Treści Serwisu).

#### Jak mogę korzystać z RSS-ów na swoim komputerze?

Do odczytywania wiadomości RSS służą specjalne programy, zwane czytnikami (patrz linki obok), przypominające zazwyczaj programy pocztowe. Są wręcz takie, które instalują się jako "wtyczka" do Twojego ulubionego programu pocztowego, dzięki czemu nie musisz uczyć się nowych programów - odczytujesz wiadomości jak zwykle e-maile. Dzięki takiemu podejściu czytnik może zaznaczać, które wiadomości już przeczytałeś i porządkować je według wybranych przez Ciebie kryteriów. Ponieważ RSS to standard przekazywania danych, a nie ich sposobu pokazywania, są też wymyślne czytniki wyświetlające na ekranie ruchomy pasek z najnowszymi wiadomościami albo np. okienko wyskakujące gdy na świecie wydarzy się coś ważnego związanego z wybranym przez Ciebie tematem zainteresowań - zależy to tylko od pomysłowości twórców oprogramowania.

36. **Spoleczność internetowa**, społeczność wirtualna (z ang. virtual community, e-community, online community) jest to zbiorowość ludzi, w której interakcje odbywają się za pośrednictwem Internetu.

Typowe społeczności internetowe powstają w oparciu o:

- grupy dyskusyjne (Usenet),
- e-mailowe listy dyskusyjne (ang. mailing list),
- fora dyskusyjne,
- kanały IRC,
- czaty,
- portale lub wortale internetowe (np. Flickr),
- blogi.

Powstanie liczących się polskich portali społecznościowych datowane jest na lata 2004 - 2006 (nasza-klasa.pl, grono.net). Od tej pory polska sieć rozwija się właśnie w kierunku portali integrujących funkcje zarówno forum, jak i czatów, list dyskusyjnych i multigalerii. Zapoczątkowana na zachodzie Europy moda porwała Polaków, którzy tworzą społeczności wielu milionów użytkowników.

37. **Blog** (ang. web log dziennik sieciowy) — rodzaj strony internetowej zawierającej określoną liczbę odrębnych, samodzielnych, uporządkowanych chronologicznie wpisów, których twórcą jest właściciel bloga. Blogi umożliwiają zazwyczaj archiwizację oraz kategoryzowanie wpisów, a także komentowanie wpisów przez czytelników danego bloga. Ogół blogów traktowany jako medium komunikacyjne nosi nazwę blogosfery.

Blogi najczęściej mają charakter osobisty i służą jako internetowe pamiętniki. Takie blogi zawierają osobiste przemyślenia, uwagi, komentarze, rysunki, a nawet nagrania - przedstawiają w ten sposób światopogląd autora. Blogi mają też wiele innych zastosowań: mogą być używane jako wortale poświęcone określonej tematyce, narzędzia marketingu czy komunikacji (np. politycznej). O ile blogi osobiste mają zazwyczaj jednego autora, o tyle w innych przypadkach blog ma często wielu autorów. Używane są też jako strony internetowe; często opatruje się je aliasami, by darmowa strona internetowa wyglądała profesjonalnie.

Autorzy blogów śledzą zazwyczaj inne blogi, tworzą do nich odsyłacze i nawiązują kontakty z ich autorami, wtedy siatka blogów zaczyna działać jako większa, powiązana całość, czyli tzw. blogosfera. W przypadku blogów poświęconych specyficznej tematyce wymiana myśli między autorami może sprzyjać rozwojowi danej dziedziny wiedzy. W przypadku blogów osobistych autorzy nawiązują często stosunki towarzyskie, dlatego też możemy porównać sieć blogów z aplikacjami rodzaju social networking, takich jak Friendster czy polskie Grono.

38. **Bezpieczeństwo danych** (ang. data security).

Działania, których celem jest ochrona danych znajdujących się w komputerach przed utratą

i niewłaściwym wykorzystywaniem. Przed umyślną lub przypadkową stratą danych chroni wykonywanie kopii zapasowych; niewłaściwemu wykorzystaniu danych przeciwdziała ograniczenie dostępu do danych, np. za pomocą ograniczenia uprawnień do wykonywania niektórych operacji na danych. Bezpieczeństwo danych ma podstawowe znaczenie dla systemów baz danych.

Działania podejmowane w celu ochrony danych w sieciach komputerowych, dostępnych w komputerach przyłączonych do sieci i danych przesyłanych między komputerami. Podstawowym sposobem ochrony danych w sieciach komputerowych jest ich szyfrowanie. Ponadto podejmowane są działania ograniczające dostęp do ważnych danych, np. są one przechowywane poza siecią, do której jest dostęp z sieci Internet.

39. **Bezpieczeństwo w sieci** – podręcznik strona **118**, rozdział **6**. Korzystanie z usług internetowych – przepisy ograniczenia i ostrzeżenia.

40. **Ergonomia** (gr. εργον - praca + νομος - prawo) - nauka o pracy czyli dyscyplina naukowa zajmująca się dostosowaniem pracy do możliwości psychofizycznych człowieka. Ma na celu humanizowanie pracy poprzez taką organizację układu: człowiek - maszyna - warunki otoczenia, aby wykonywana ona była przy możliwie niskim koszcie biologicznym i najbardziej efektywnie, co uzyskuje się m.in. poprzez eliminację źródeł chorób zawodowych. Ergonomia jest nauką interdyscyplinarną. Korzysta z dorobku takich nauk lub dziedzin naukowych jak: psychologia pracy, socjologia pracy, fizjologia pracy, higiena, medycyna pracy, organizacja pracy, antropometria oraz nauk technicznych, np. materiałoznawstwa, budowy maszyn.

Twórcą pojęcia "ergonomia" (z gr. ergon - praca, nomos - zasada, prawo) jest Wojciech Jastrzębowski, który zdefiniował ergonomię jako naukę o używaniu nadanych człowiekowi od Stwórcy sił i zdolności.

Przedmiotem badań jest układ człowiek - maszyna - warunki materialnego otoczenia pracy - warunki pracy na stanowisku roboczym. Celem głównym jest polepszanie warunków pracy człowieka, które obejmuje dostosowanie ich do możliwości pracownika oraz właściwy dobór pracownika do danej pracy i jego edukację obejmującą specyfikę stanowiska.

Wyróżnia się ergonomię koncepcyjną (wprowadzanie zasad ergonomii podczas opracowania koncepcji oraz projektowania) i ergonomię korekcyjną (korektę warunków pracy na drodze modernizacji już funkcjonujących stanowisk pracy (maszyn, urządzeń).

41. **Wpływ oświetlenia na komfort pracy przy komputerze.**

Według zaleceń specjalistów, idealnie ustawione stanowisko komputerowe powinno znajdować się na bezkiennej ścianie, bokiem do okna, by światło padało z lewej strony, i w odległości nie mniejszej niż 1 metr. Ogólna zasada jest taka, że na ekranie monitora nie może się odbijać światło (refleksy świetlne mają negatywny wpływ na wzrok, oczy się szybciej i bardziej dotkliwie męczą). Oprawy oświetlenia ogólnego powinny być skierowane tak, by światło padało na podłogę lub blat stołu (nigdy na ekran monitora!). Ustawiając monitor na biurku należy zwrócić uwagę, by górny brzeg ekranu znajdował się nieco poniżej poziomu oczu, nigdy powyżej. Człowiek przy komputerze powinien siedzieć tak, by mniej więcej środek monitora znajdował się na wysokości jego wzroku.

Pomieszczenie, w którym pracują komputery powinno być często wietrzone lub być wyposażone w klimatyzację. Należy zadbać także o obecność roślin doniczkowych, najlepiej paproci.

42. **Open Source** – (otwarte oprogramowanie), to odłam ruchu wolnego oprogramowania, który dąży do tego, aby istniał swobodny i wolny dostęp do oprogramowania dla wszystkich użytkowników.

Open Source jest oprogramowaniem, którego licencja pozwala na legalne i darmowe kopiowanie, kodu wynikowego, źródłowego oraz na dowolne jego modyfikacje.

Istnieje kilka kryteriów, które musi spełnić oprogramowanie, by zakwalifikowało się ono jako otwarte. Najważniejsze z nich to: wolna dystrybucja, kod źródłowy rozpowszechniany z programem, integralność kodów źródłowych autora, rozpowszechnianie licencji, licencja nie musi być szczegółna dla produktu, ani wpływać na inne oprogramowanie.

Dzięki temu, że programy objęte licencją Open Source udostępniają swobodni dostępu do kodów źródłowych (np. przez Internet), może być one udoskonalane i rozpowszechniane przez ludzi na całym świecie, co pociąga za sobą szybki rozwój programów oraz wysoką wykrywalność wszelkich błędów.

#### **Popularne oprogramowanie Open Source:**

- 7-zip - kompresja danych.
- Azureus - klient sieci Torrent.
- ClamWIN - antywirus.
- eMule - klient sieci ed2k.
- FileZilla - akcelerator pobierania plików.
- Firefox - przeglądarka internetowa.
- GIMP - edytor grafiki.
- Linux - system operacyjny.
- Nvu - graficzny edytor HTML.
- OpenOffice.org - pakiet biurowy.
- Thunderbird - klient pocztowy.
- XviD - kodek.<sup>1</sup>

#### **43. Umiejętność oszczędzania energii elektrycznej przy pracy związanej z użyciem komputera.**

„A ile komputer może zużyć prądu?” . Okazuje się, że całkiem sporo. W skali roku opłaty za energię elektryczną związane z używaniem komputera mogą przekroczyć 500 zł. Redakcja PC Worlda zadała sobie trud i rozprawiła się z pięcioma mitami dotyczącymi oszczędzania energii w domowym komputerze.

##### **1. mit: częste wyłączenie komputera skraca jego życie**

Nieprawda. Jest to uogólnienie, którego nie potwierdzają badania. Jeżeli nie korzystamy z komputera lepiej go wyłączyć. Mniej będzie się zużywał m.in. dysk twardy.

##### **2. mit: dużo rdzeni procesora, to większy pobór energii**

Czasami tak, czasami nie. Dzięki zwiększeniu ilości rdzeni nie trzeba podkreślać procesora. Nowoczesne urządzenia mają systemy, które obniżają ich moc podczas mniejszych obciążeń. Pozwala to na cichszą pracę komputera i mniejszy pobór prądu.

##### **3. mit: monitor LCD zużywa o wiele mniej energii niż CRT**

To prawda. Trzeba jednak pamiętać, że wraz ze wzrostem jego przekątnej pobór prądu rośnie. Jeżeli więc wymienimy stary monitor na znacznie większy LCD może się okazać, że nasze zużycie energii wzrośnie. W trakcie czuwania nowoczesny monitor pobiera w granicach 1 W.

##### **4. mit: drukarka może być włączona cały czas, bo zużywa prąd tylko w trakcie drukowania**

Nieprawda. Drukarka zużywa bardzo dużo energii w trakcie drukowania, ale w przypadku drukarki laserowej ten moment trwa kilkadziesiąt sekund. Natomiast w trybie czuwania cały czas pobiera energię – ok. 20 W. W skali miesiąca więcej wydamy na prąd zużyty na czuwanie niż drukowanie. Wyłączajmy drukarki!

##### **5. mit: systemy oszczędzania energii instalowane na płytach głównych nie działają**

Nieprawda. Systemy działają, a skala oszczędności zależy od konkretnego modelu urządzenia.

Czy jest się o co bić? Ile tak naprawdę kosztuje nas korzystanie z komputera? Okazuje się, że całkiem sporo. Jeżeli założymy, że przez 16 godzin na dobę mamy włączony domowy zestaw składający się z komputera, monitora LCD, laptopa, drukarki ze skanerem, dysku sieciowego i routera ADSL, to przez rok wydamy przeszło 500 zł na zasilanie tych urządzeń.

#### **44. Zasady zabezpieczania danych.**

Nie ma sensu funkcjonowanie żadnego systemu informatycznego, jeśli przetwarzane w nim dane nie są właściwie chronione. Ochrona tych danych powinna być kompleksowa, spójna i odpowiadająca

---

<sup>1</sup> <http://www.open-source.eprogramy.net/>

potrzebom przedsiębiorstwa. Zagadnienia dotyczące ochrony danych w przedsiębiorstwie powinny być ujęte w dokumencie polityki bezpieczeństwa (*nie tylko informatycznego*).

W każdym przypadku strategię ochrony danych w firmie należy opracowywać, biorąc pod uwagę wewnętrzną strukturę firmy, szybkość jej wzrostu, posiadane przez nią środki finansowe i wiele innych, indywidualnych czynników. Ale same najlepsze zabezpieczenia nie wystarczą, jeśli użytkownicy nie będą świadomi wartości swoich danych. Nie dadzą nic również, jeśli sprzęt nie będzie stosowany zgodnie ze zdrowym rozsądkiem. Według danych Interpolu (*ale informacje te potwierdzają też analitycy rynku*) co drugie zagrożenie systemu IT i danych jest powodowane nieumyślnym błędem człowieka. Co czwarte to celowe działanie pracowników.

Tworzenie dokumentu polityki bezpieczeństwa to nie tylko zbiór zagadnień natury czysto informatycznej. Konieczne są do tego także elementy wiedzy na temat tzw. inżynierii społecznej (*social engineering*). Wiedzę tę z reguły potrafią wykorzystać osoby atakujące system. Starają się uzyskać jak najwięcej informacji o firmie lub jej pracownikach oraz spowodować, żeby działali oni w sposób oczekiwany przez atakującego. Niestety, naiwność ludzka w tej kwestii jest jeszcze bardzo duża – wystarczy prześledzić liczbę rozsyłanych pocztą elektroniczną fałszywych alarmów wirusowych.

Wśród wielu zagadnień, które porusza dokument polityki bezpieczeństwa, powinny znaleźć się też tematy dotyczące pamięci masowych. Oto niektóre z nich:

- regularne tworzenie kopii bezpieczeństwa;
- sprawdzenie poprawności algorytmów wykonywania kopii;
- przechowywanie i regularna rotacja zestawu kopii bezpieczeństwa poza siedzibą firmy - uchroni to dane przed skutkami lokalnych katastrof;
- dostęp do kopii bezpieczeństwa ograniczony tylko dla właściwych osób;
- regularne próby odtwarzania całego systemu na serwerze testowym;
- instalacja oprogramowania antywirusowego i regularna aktualizacja definicji wirusów;
- właściwy opis nośników z kopiami zapasowymi;
- określenie procedury postępowania w razie awarii napędu;
- przygotowanie i aktualizacja awaryjnego zestawu naprawczego zawierającego dysk startowy, oprogramowanie diagnostyczne, wersję instalacyjną systemu operacyjnego, wersję instalacyjną programu do zabezpieczania danych, aktualne wersje sterowników, odpowiednie narzędzia i zapasowe media.

Po wprowadzeniu w życie wszystkich tych procedur firma będzie mogła powiedzieć o chronionym systemie, że jest przynajmniej godny zaufania. Do pełnego bezpieczeństwa prawdopodobnie będzie mu i tak wiele brakować - osiągnięcie tego stanu jest po prostu niemożliwe.

#### 45. **Zapora sieciowa** (ang. *firewall* – ściana ogniowa) – jeden ze sposobów zabezpieczania sieci i systemów przed intruzami.

Termin ten może odnosić się zarówno do dedykowanego sprzętu komputerowego wraz ze specjalnym oprogramowaniem, jak i do samego oprogramowania blokującego niepowołany dostęp do komputera, na którego straży stoi. Pełni rolę połączenia ochrony sprzętowej i programowej sieci wewnętrznej LAN przed dostępem z zewnątrz tzn. sieci publicznych, Internetu, chroni też przed nieuprawnionym wpływem danych z sieci lokalnej na zewnątrz. Często jest to komputer wyposażony w system operacyjny (np. Linux, BSD) z odpowiednim oprogramowaniem. Do jego podstawowych zadań należy filtrowanie połączeń wchodzących i wychodzących oraz tym samym odmawianie żądań dostępu uznanych za niebezpieczne.

Najczęściej używanymi technikami obrony są:

- Filtrowanie pakietów, czyli sprawdzanie pochodzenia pakietów i akceptowanie pożądaných (np. SPI).
- Stosowanie algorytmów identyfikacji użytkownika (hasła, cyfrowe certyfikaty).
- Zabezpieczanie programów obsługujących niektóre protokoły (np. FTP, TELNET).

Bardzo ważną funkcją zapory ogniowej jest monitorowanie ruchu sieciowego i zapisywanie najważniejszych zdarzeń do dziennika (logu). Umożliwia to administratorowi wczesne dokonywanie



zmian konfiguracji. Poprawnie skonfigurowany firewall powinien odeprzeć wszelkie znane typy ataków. Na zaporze można zdefiniować strefę ograniczonego zaufania – podsieć, która izoluje od wewnętrznej sieci lokalne serwery udostępniające usługi na zewnątrz.

#### Typy zapór sieciowych

- **Zapory filtrujące:** monitorują przepływające przez nie pakiety sieciowe i przepuszczają tylko zgodne z regułami ustawionymi na danej zaporze (zapora pracująca dodatkowo jako router). Zwykle w niewielkich sieciach jest zapora sprzętowa bądź wydzielony komputer z systemem operacyjnym Linux. Obecnie najczęściej wykorzystywana metoda filtrowania w Linuksie to reguły oparte na iptables. Dostępne są także zamknięte komercyjne rozwiązania programowe, z których wiele posiada bardzo wymyślne własności i rozbudowany system konfiguracji oraz wachlarz możliwych do zintegrowania rozwiązań, pozwalających nie tylko na analizę (Snort, psad) i filtrowanie pakietów IP, ale także na sprawdzanie poprawności pakietów z punktu widzenia wyższych warstw modelu ISO/OSI, a nawet na prowadzenie ochrony antywirusowej.
- **Oprogramowanie komputerów stacjonarnych:** udostępnia wybrane porty do połączeń „z zewnątrz” monitorując ruch, udostępnia także połączenia na zewnątrz komputera wybranym usługom/programom. Często zintegrowane z ochroną antywirusową (na przykład Norton Internet Security).
- **Zapory pośredniczące (proxy):** wykonujące połączenie z serwerem w imieniu użytkownika. Przykładowo, zamiast uruchomienia sesji http bezpośrednio do zdalnego serwera WWW, uruchamiana jest sesja z zaporą i dopiero stamtąd uruchamiane jest połączenie z systemem zdalnym. Cała komunikacja na serwer http przechodzi przez *proxy*, które może filtrować ruch. *Proxy*, jeśli ma taką funkcjonalność, potrafi rozpoznać komendy http jak i analizować zawartość pobieranych stron WWW (działa w warstwie aplikacji modelu ISO/OSI). Zabezpieczające działanie zapory, z punktu widzenia klienta, polega w tym wypadku na tym, iż możliwe jest blokowanie wybranej treści (ang. *content filtering*), aby nie dotarła ona do klienta (np. strony ze słowami wulgarnymi, o treści pornograficznej itp.).

Współcześnie często pracująca zapora sieciowa jest rozwiązaniem hybrydowym analizującym pakiety od warstwy łącza danych do aplikacji modelu OSI. Umożliwia realizację złożonych polityk bezpieczeństwa oraz integrację z systemami IDS.

46. **Wirus komputerowy** – najczęściej prosty program komputerowy, który w sposób celowy powiela się bez zgody użytkownika. Wirus komputerowy w przeciwieństwie do robaka komputerowego do swojej działalności wymaga nosiciela w postaci programu komputerowego, poczty elektronicznej itp. Wirusy wykorzystują słabość zabezpieczeń systemów komputerowych lub właściwości systemów oraz niedoświadczenie i bez troskę użytkowników.

Wirus komputerowy to krótki program komputerowy, zwykle szkodzący systemowi operacyjnemu lub utrudniający pracę użytkownikowi komputera. Każdy wirus ma zdolność samopowielania. Jest to warunek konieczny, aby dany program można było nazywać wirusem.

Wirusy przenoszone są przeważnie w zainfekowanych wcześniej plikach (wirusy plikowe) lub w pierwszych sektorach fizycznych (na zerowej ścieżce) dysku twardego (wirusy dyskowe). Proces infekcji polega na odpowiedniej modyfikacji struktury plików lub sektorów. Zainfekowaną ofiarę nazywa się nosicielem, a proces samopowielania replikacją.

Długość typowego wirusa w czasach panowania DOS-u wahała się w granicach od kilkudziesięciu bajtów do kilku kilobajtów, choć już wtedy były wirusy o rozmiarze kilkudziesięciu kilobajtów. Obecnie klasyczne wirusy spotyka się rzadziej – częściej jest to hybryda wirusa z robakiem, a rozmiar kilkadziesiąt i więcej kilobajtów nie dziwi – tyle kodu bez problemu można ukryć w wielomegabajtowych bibliotekach czy programach. Rozmiar wirusa zależy od czynników takich jak:

- umiejętności programistyczne twórcy wirusa – wirus lepszego programisty napisany w tym samym języku będzie mniejszy lub będzie miał więcej funkcji;
- użyty język programowania – wirus o podobnej funkcjonalności napisany w języku maszynowym (assembler) zwykle będzie mniejszy niż w języku skryptowym czy języku wysokiego poziomu;

- przewidywana funkcjonalność wirusa – prosty wirus będzie mniejszy od szkodnika wykonującego wiele różnych czynności; najmniejsze wirusy potrafią tylko się powielać;
- wykorzystanie cech środowiska operacyjnego – wirus napisany jako maksymalnie niezależny musi mieć wbudowane wszystkie potrzebne biblioteki, wirus korzystający w pełni ze środowiska ma tylko minimum kodu niezbędne do wywołania dostępnych w tym środowisku funkcji.

Od programisty zależą także efekty, jakie wirus będzie wywoływał po zainfekowaniu systemu, na przykład:

- kasowanie i niszczenie danych,
- rozsyłanie spamu,
- dokonywanie ataków na serwery internetowe,
- kradzież danych (hasła, numery kart płatniczych, dane osobowe),
- wyłączenie komputera,
- wyświetlanie grafiki lub odgrywanie dźwięków,
- uniemożliwienie pracy na komputerze,
- umożliwienie przejęcia kontroli nad komputerem osobie nieupoważnionej,
- tworzenie botnetu.

**47. Program antywirusowy.** Program służący do wykrywania wirusów. Na ogół ten sam program usuwa wykryte wirusy. Ze względu na szybkie wprowadzanie do obiegu coraz to nowych wirusów zaleca się, by taki program był często uaktualniany. W większości przypadków można to robić korzystając z sieci Internet.

Rośnie nie tylko liczba wirusów, ale rozszerza się również ich zakres działania. Niektóre z nich przenoszą się na przykład wraz listami elektronicznymi i infekują komputer podczas odczytywania korespondencji. Aby temu zapobiegać, programy antywirusowe są rozszerzane o tzw. monitor - program, który jest aktywny przez cały czas pracy komputera i bez ingerencji użytkownika sprawdza, czy w czasie wykonywania operacji na zewnętrznych nośnikach (np. w czasie uaktywniania dyskietki) i plikach (np. pochodzących z sieci) nie przedostaje się do komputera jakiś wirus.

Zaleca się, by program antywirusowy był uruchamiany przy każdym korzystaniu z obcych i nieznanych plików oraz obcych nośników (takich, jak dyskietki i płyty CD). Ponadto przez cały czas powinien być aktywny monitor takiego programu.

Najbardziej znanym polskim programem antywirusowym jest Mks\_Vir. Jest on wyposażony w monitor i można go uaktualniać za pośrednictwem sieci Internet (zob. <http://www.mks.com.pl>).

**48. Prawa autorskie** – zbiór przepisów prawa dotyczących ochrony praw autorów dzieł takich, jak: książki, filmy, piosenki, utwory muzyczne, utwory sceniczne, obrazy malarstwa, grafiki, a także programy komputerowe. W Polsce od 1994 roku obowiązuje nowa ustawa o prawie autorskim. Fragmenty tej ustawy (rozdz. 7 i 15) są poświęcone prawu komputerowemu, czyli ochronie praw twórców oprogramowania.

Prawo autorskie zapewnia, że rozpowszechnianie (np. piosenek za pośrednictwem radia), kopiowanie (np. książek lub programów komputerowych) lub sprzedaż utworów objętych tym prawem służy autorom i przynosi im zyski.

**49. Prawo komputerowe** (ang. computer law). Zbiór przepisów dotyczących ochrony i rozpowszechniania oprogramowania, wynikających z ogólniejszych przepisów prawa autorskiego o ochronie własności intelektualnej. Program komputerowy, zgodnie z ustawą o prawie autorskim z 1994 roku, został uznany za własność intelektualną.

Nabywca programu komputerowego drogą legalną otrzymuje od producenta oprogramowania licencję, która określa warunki jego użytkowania. Duże instytucje, takie jak szkoły, nabywają często oprogramowanie z licencją strefową, która zezwala na korzystanie z tego oprogramowania na wszystkich komputerach tej instytucji.

Prawo komputerowe jest jednak nagminnie łamane, zarówno przez użytkowników indywidualnych, jak i przez całe instytucje.

Na rynku są dostępne programy, które nie w pełni podlegają ograniczeniom prawa komputerowego:

programy do publicznego rozpowszechniania, programy bezpłatne i programy typu shareware.

50. **Shareware** to rodzaj licencji programu komputerowego, który jest rozpowszechniany bez opłat z pewnymi ograniczeniami lub z niewielkimi opłatami do wypróbowania przez użytkowników. Czasami po okresie próbnym (wersja trial) lub po określonej liczbie uruchomień (limit uruchomień) za taki program trzeba płacić lub zrezygnować z korzystania z niego.

Czasami producent oprogramowania wydaje jedną wersję na licencji shareware, a drugą (zazwyczaj z ograniczeniami, np. z blokadą dostępu do niektórych funkcji) na licencji freeware.

51. **Przetwarzanie danych osobowych** to termin prawniczy, który w prawie polskim został zdefiniowany w ustawie dnia 29 sierpnia 1997 roku o ochronie danych osobowych (t.j. Dz.U. z 2002 r. Nr 101, poz. 926 ze zm.) (ustawodawca posłużył się określeniem przetwarzanie danych). Przetwarzanie oznacza jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

Dane osobowe można przetwarzać w ściśle określonych przez prawo sytuacjach (art. 23 ustawy o ochronie danych osobowych):

- osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie tych danych,
- jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,
- jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,
- jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,
- jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Istnieje generalny zakaz przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym z wyjątkiem sytuacji ściśle określonych przepisami.

Za zgodne z prawem przetwarzanie danych osobowych odpowiada administrator danych osobowych, który może wyznaczyć administratora bezpieczeństwa informacji nadzorującego przestrzeganie przepisów w zakresie ochrony danych osobowych.

52. **Budowa komputera – główne części komputera.**

Obudowa – skrzynia, wewnątrz której zamontowany jest zasilacz, wentylator chłodzący oraz podzespoły komputera, które wymienię i opiszę poniżej. Obudowy różnią się od siebie rozmiarami i kształtem:

1. Tower – (Stojąca) – istnieją trzy rodzaje tych obudów różniące się między sobą wysokością, a więc i pojemnością:

♣ Mini-tower – najmniejsza, można zainstalować dwa małe napędy, np. napęd dyskietek 3,5” i dwa duże, np. napędy CD-ROM.

♣ Midi-tower – jest nieco wyższa i zazwyczaj pozwala na zamontowanie z przodu trzech napędów dużych i dwóch małych

♣ .Big-tower – największa, ma pięć miejsc na duże napędy i zwykle dwa na małe. W środku jest sporo miejsca na zamontowanie dodatkowych dysków twardych. Rzadko spotykana w zastosowaniach domowych. Służy ona raczej do konstrukcji serwerów.

2. Desktop - (Płaska) – skonstruowana w taki sposób, aby było można na niej postawić monitor. Zwykle obudowy te mają mało miejsca na dodatkowe urządzenia, takie jak np. nagrywarka CD-RW. W firmowych komputerach dodatkowych miejsc z przodu obudowy nie ma w ogóle, przez co nie można ich rozbudować.

- Z pośród elementów składowych komputera (znajdujących się w obudowie) należy wymienić:
- Mikroprocesor.
- Płyta główna.
- Pamięć operacyjna (RAM).
- Dysk twardy.
- Napęd dyskietek.
- Napęd (CD-ROM, DVD-ROM) oraz nagrywarka (CD-RW, DVD-RW) przeważnie jedno z tych urządzeń.
- Karty rozszerzeń: graficzna, dźwiękowa, (ewentualnie inne – stosownie do potrzeb).
- Modem

Mikroprocesor, zwany również procesorem – jest to układ scalony, który wykonuje zadania zleczone komputerowi-jego rolę można porównać do mózgu człowieka. Procesor nadzoruje i synchronizuje prace wszystkich urządzeń w komputerze. Jest kilka charakterystycznych cech, które odróżniają procesory od siebie: architektura (CISC - starszej generacji, wyposażone w pełen zestaw instrukcji lub RISC – najnowocześniejsze i najbardziej wydajne, ze zredukowanym zestawem instrukcji), liczba bitów przetwarzanych w jednym cyklu, częstotliwość taktowania podawana w MHz. Procesor montuje się na płycie głównej w specjalnym gnieździe zwanym socket. Cechą procesora jest to, iż w czasie pracy wytwarza dużą ilość ciepła i dlatego należy zamontować na nim wentylator, który to ciepło odprowadzi.

Płyta główna – najczęściej prostokątna płyta stanowiąca podłoże, na którym umieszcza się układy elektroniczne komputera, takie jak procesor, pamięć RAM czy karty rozszerzeń. Na współczesnych płytach głównych zintegrowane są wszystkie standardowe interfejsy komputera, od portów szeregowych i równoległych po USB. Poza tym należałoby wyróżnić:

- Kontroler – układ scalony, który, dba o komunikację między urządzeniami znajdującymi się poza obębem płyty głównej.
- Chipset – kontroluje przepływ danych (bitów) pomiędzy poszczególnymi podzespołami podłączonymi do płyty głównej.
- Pamięć ROM – pamięć jedynie do odczytu, podtrzymywana długowieczną baterią zamontowaną również na płycie głównej. W pamięci ROM zapisane są standardowe (fabryczne) ustawienia Biosu (testuje sprzęt po włączeniu komputera, uruchamia system operacyjny, kontroluje transfer danych pomiędzy komponentami takimi jak dysk twardy, procesor czy napęd CD-ROM).
- Gniazda – po przez które podłączamy do płyty głównej elementy naszego komputera.

Pamięć operacyjna RAM – pamięć o dostępie bezpośrednim lub swobodnym, do której komputer ładuje aktualnie używane dane tak, aby były one błyskawicznie dostępne dla procesora. Obecnie wyróżniamy dwa rodzaje pamięci RAM:

- SDRAM – rodzaj szybkiej synchronicznej pamięci RAM, o bardzo krótkim czasie dostępu (nawet 5,5 ns) stosowana w komputerach zarówno jako pamięć RAM, jak i pamięć do kart graficznych. Montuje się ją na płycie głównej w postaci modułów DIMM (jest to płytka drukowana, na której umieszczone są układy scalone).
- DDR-SDRAM – skrótowo nazywane pamięciami DDR charakteryzuje się dwukrotnie większą szybkością działania niż tradycyjne moduły SDRAM.

W przeciwieństwie od pamięci ROM pamięć RAM do funkcjonowania potrzebuje stałego źródła zasilania, co wiąże się z tym, iż po wyłączeniu komputera dane w niej zawarte giną.

Dysk twardy – element komputera służący do trwałego przechowywania danych (zostają one na nim również po wyłączeniu komputera). We wnętrzu dysku twardego znajdują się talerze (w większości dysków od dwóch do ośmiu), pokryte materiałem magnetycznym, nad którymi umieszczone są głowice zapisujące i odczytujące dane. Talerze wirują z prędkością tysięcy obrotów na minutę, dzięki czemu czas dostępu do informacji jest krótki, a szybkość transferu danych wysoka. Dużą zaletą twardych dysków jest ich duża pojemność liczona w gigabajtach.

Napęd dyskietek – urządzenie elektromechaniczne, które może odczytywać i zapisywać dane na dyskietkach magnetycznych. Obecnie stosowane napędy to napędy dyskietek 3,5-calowych,

mogących pomieścić 1,44 Mb danych.

Napęd CD-ROM – umożliwia komputerowi odczytywanie płyt CD-ROM, CD, CD-R i CD-RW. Podczas odczytu na dysk znajdujący się w napędzie CD-ROM pada światło lasera. Informacje o odbiciu lub nie odbiciu światła lasera są przekazywane do komputera w postaci jedynki i zera, tworząc bity danych. Czas dostępu do informacji w typowych napędach CD-ROM wynosi 90-120 ms, czyli jest ok. 10 razy dłuższy niż dla dysków twardych. Prędkość odczytu określa się jako wielokrotność prędkości pierwszego napędu tego typu (oznaczonej jako x1) 150kB/s. Tak, więc napęd CD-ROMx50 powinien odczytywać dane z maksymalną szybkością transferu 7,3MB/s.

Napęd DVD-ROM – umożliwia komputerowi odczytywanie płyt DVD i DVD-ROM, a także zwykłych płyt CD-ROM, CD, CD-R i CD-RW. Zasada działania napędu jest taka sama jak napędu CD-ROM, różnica polega na wykorzystaniu innego typu lasera. Napędy DVD-ROM działają obecnie z szybkością transferu od 1,3MB/s (x1) do 20,8MB/s (x16). Dla napędu DVD-ROM przyjęto podstawową prędkość odczytu(x1) na poziomie 1,3MB/s.

Nagrywarka CD-RW – spełnia rolę napędu CD-ROM, oraz dodatkowo może nagrywać płyty CD-R i CD-RW. Nagrywarki CD-RW używają trzech różnych mocy lasera:

- Najwyższej – do zapisu (laser przekształca fragment powierzchni płyty do stanu amorficznego, a więc nieodbijającego światła).
- Średniej – do wymazywania danych ( laser przekształca fragment powierzchni płyty z powrotem do stanu krystalicznego, w którym ta odbija światło).
- Najniższej – do odczytu (Laser nie powoduje zmian strukturalnych powierzchni).

Nagrywarka DVD – urządzenie o funkcjonalności zbliżonej do nagrywarki CD-RW, które może także zapisywać dane, w co najmniej jednym z trzech niekompatybilnych ze sobą standardów nagrywania płyt DVD – DVD-RAM, DVD-R(DVD-RW) i DVD+R(DVD+RW). Obecnie najnowsze nagrywarki DVD nagrywają we wszystkich trzech standardach.

Karty rozszerzeń:

- Karta graficzna – jej zadaniem jest przetwarzanie danych podawanych przez komputer do postaci zrozumiałej dla monitora. Karty graficzne różnią się między sobą szybkością pracy, wielkością pamięci RAM, wyświetlaną rozdzielczością obrazu, liczbą dostępnych kolorów oraz częstotliwością odświeżania. Najnowsze karty graficzne wyposażone są w akceleratory 3D.
- Karta dźwiękowa - pozwalająca na odgrywanie oraz nagrywanie na komputerze dźwięku w formie plików muzycznych, umożliwia także podłączenie do nich głośników, wzmacniacza, mikrofonu oraz urządzeń MIDI. Obecnie większość płyt głównych jest zintegrowana z kartą dźwiękową. Istnieje jednak możliwość zamontowania karty dźwiękowej na płycie głównej dla uzyskania lepszych parametrów przetwarzanego dźwięku niż oferuje to karta zintegrowana z płytą główną.

Modem – urządzenie, które przetwarza cyfrowe dane na postać analogową po to, aby można je przesłać do innego modemu z użyciem standardowej linii telefonicznej. Modem może również zmieniać fale analogowe z powrotem na postać cyfrową i przekazywać je do komputera. Niedogodności tej pozbawione są urządzenia nazwane adapterami ISDN. Produkowane są dwa rodzaje modemów: wewnętrzne i zewnętrzne. Modemy różnią się między sobą poza tym szybkością transmisji – najszybsze z nich pracują z szybkością 56 kaps.. Właśnie po przez zastosowanie modemu mamy dostęp do Internetu.

Aby nasz komputer mógł działać należy zainstalować na początek system operacyjny. Nie będzie jednak to możliwe bez podłączenia do jednostki centralnej dodatkowych urządzeń zewnętrznych dzięki którym będziemy mogli wprowadzać i odczytywać (w różnej postaci - obraz, dźwięk, wydruk) dane.

Urządzenia zewnętrzne możemy podzielić na:

1. Wejściowe
2. Wyjściowe

Urządzenia wejściowe to:

- Klawiatura
- Myszka
- Skaner

- Aparat fotograficzny – cyfrowy, kamera cyfrowa.

Klawiatura – typowa klawiatura składa się z klawiszy maszynowych, odpowiadają one literom, cyfrom i znakom przestankowym, klawiszy funkcyjnych oznaczonych od F1 do F12, klawiszy numerycznych odpowiadających układowi kalkulatora i klawiszy kursora, które służą do przesuwania na ekranie kursora. Klawiatura pozwala na wpisywanie tekstu i liczb. Klawisze specjalne służą do przekazywania poleceń lub do sterowania czynnościami na ekranie monitora. Klawiatura podłączona jest do komputera za pomocą kabla, choć występują również klawiatury komunikujące się z komputerem za pomocą podczerwieni lub drogą radiową.

Myszka – niewielkie urządzenie podłączone za pomocą kabla (nie dotyczy myszek bezprzewodowych) do komputera, które przesuwamy po płaskiej powierzchni w celu uzyskania ruchu kursora na ekranie monitora. Standardowa mysz składa się z plastikowej obudowy kryjącej w sobie wystającą przez otwór w jej podstawie kulkę. Informacje o przesuwie kulki dostarczane są do komputera, gdzie aktywny program na ich podstawie w tym samym czasie przesuwa kursor na ekranie monitora zgodnie z ruchem urządzenia. Obecna mysz wyposażona jest zazwyczaj w dwa przyciski i rolkę:

- Lewy przycisk – znacznie częściej używany i odpowiada za typowe zadania, np. uruchomienie programu, otwarcie folderu.
- Prawy przycisk – używany rzadziej służy zazwyczaj do otwierania menu kontekstowego.
- Rolka – zazwyczaj znajduje się pomiędzy przyciskami, służy do przewijania wielostronicowych dokumentów (np. stron WWW).

Aktualnie na rynku dostępne są myszki, które zamiast kulki posiadają układ optyczny analizujący obraz powierzchni, po której przesuwana jest mysz - nazywamy je myszkami optycznymi. Występują również myszki bezprzewodowe, które przesyłają dane do komputera za pomocą podczerwieni lub drogą radiową.

Natomiast z pośród urządzeń wyjściowych można wymienić:

- Monitor
- Drukarka
- Głośniki

Monitor - Żaden komputer nie nadaje się do pracy bez monitora czy wyświetlacza. Najczęściej jest to monitor kolorowy, przypominający mały telewizor. Instrukcje dotyczące tego, co ma być wyświetlane na jego ekranie, przekazuje mu zainstalowana w komputerze karta graficzna, która przetwarza je do postaci zrozumiałej dla monitora. Liczba wyświetlanych jednocześnie kolorów zależy od możliwości zainstalowanej w komputerze karty graficznej. Obecnie spotykamy dwa typy monitorów:

- CRT – monitor wyposażony w lampę kineskopową, mają one bardzo dobre parametry wyświetlanego obrazu, ich wadą są jednak spore rozmiary i promieniowanie wytwarzane przez kineskop.
- LCD – monitor wyposażony w wyświetlacz ciekłokrystaliczny. Ze względu na brak kineskopu są one płaskie i zajmują bardzo mało miejsca. Ich jakość obrazu, a szczególnie ostrość jest bardzo dobra. Jeszcze jedną ich zaletą jest mniejsze zmęczenie oczu podczas długotrwałej pracy niż w przypadku monitorów CRT.

Drukarka – spełniają podobną rolę, jak monitory tyle tylko, że tekst jak i grafika pojawiają się nie na ekranie, ale na papierze. Cały proces wygląda, więc, bardzo podobnie: informacje, które mają pojawić się na papierze wysyłane są z komputera do karty drukarki. Tam zostają zmienione w obraz strony, który następnie poprzez drukarkę trafia na papier. Do zastosowań domowych nadaje się albo drukarka atramentowa, albo laserowa. Drukarki atramentowe są tańsze, lecz jednocześnie wolniejsze niż drukarki laserowe. Oba typy zapewniają jednak dość wysoką jakość druku, czasami zbliżoną do jakości czasopism. Zasada działania drukarek atramentowych polega na wytryskiwaniu małych kropeł atramentu na papier, przy czym wszystko to odbywa się praktycznie bezgłośnie. Drukarki laserowe funkcjonują na zasadzie podobnej do kserokopiarki. Strumień lasera zaznacza obraz na metalowym bębnie. W miejscach tych pozostaje sproszkowany atrament, czyli toner. Następnie do bębna dociskany jest papier, z którym toner wiąże się pod wpływem wysokiej

temperatury. Drukarki laserowe gwarantują najwyższą jakość i nadają się przede wszystkim do zastosowań graficznych i przygotowywania profesjonalnych publikacji. O jakości drukarki decydują przede wszystkim następujące parametry:

- Możliwość drukowania w kolorze.
- Rozdzielczość – liczba podana w dpi, która określa, z jaką dokładnością (wiernością) drukarka może stworzyć wydruki.
- Szybkość wydruku (liczba stron na minutę).

Głośniki – dzięki głośnikom możemy usłyszeć dane z komputera przetworzone przez kartę dźwiękową takie jak: muzykę, dźwięki podczas oglądania filmów, głos naszego rozmówcy przy prowadzeniu rozmowy poprzez Internet i tym podobne.

## 53. Telefonía VoIP

### 1. Co to jest VoIP i ile kosztuje?

VoIP (ang. Voice over Internet Protocol) to technologia przesyłania głosu z wykorzystaniem protokołu internetowego. Nazywana również telefonią internetową, wykorzystuje istniejącą infrastrukturę, jaką jest Internet. Dzięki temu operatorzy VoIP nie ponoszą kosztów utrzymania łączy telekomunikacyjnych (jak to jest w przypadku telefonii tradycyjnej), co pozwala im oferować bardzo niskie ceny połączeń w porównaniu z telefonią tradycyjną. Rozmowy przez Internet przeważnie są zupełnie darmowe.

### 2. Kto może korzystać a VoIP?

Z telefonii internetowej w pełni może korzystać praktycznie każdy, kto ma dostęp do Internetu i komputer lub specjalny terminal VoIP (bramka, telefon IP).

Aby jakość dźwięku była wysoka a co za tym idzie rozmowa komfortowa, wszyscy operatorzy telefonii VoIP zalecają szerokopasmowy dostęp (np. Neostrada).

### 3. Jak można korzystać z VoIP?

Przed rozpoczęciem użytkowania VoIP należy nieco zainwestować. O tym jaki sprzęt należy kupić, można się dowiedzieć z poniższej tabelki.

Typ dzwonięcia	Opis	Urządzenia, programy
Dzwonienie bez włączania komputera	To rozwiązanie pozwoli na korzystanie z VoIP jak z klasycznej telefonii. Będzie można dzwonić bez włączania komputera. Należy się jednak zaopatrzyć w odpowiedni sprzęt, który może kosztować od 100 zł (w zależności od typu łącza jakie mamy). Alternatywnym rozwiązaniem może być zakup telefonu IP – w zależności od modelu, możemy go podłączyć bezpośrednio do naszej przewodowej sieci LAN lub do bezprzewodowej sieci Wi-Fi.	Bramka VoIP + zwykły telefon lub telefon IP

Dzwonienie z telefonu podłączonego do komputera	Ta opcja pozwoli na korzystanie ze zwykłego telefonu bez konieczności posiadania rozbudowanej infrastruktury sieciowej w domu. Wystarczy dokupić bramkę VoIP pod USB. Innym rozwiązaniem może być specjalny telefon VoIP, należy podłączyć przez port USB bezpośrednio do naszego komputera. W tym przypadku komputer musi być włączony, a komunikator uruchomiony.	Bramka VoIP USB + zwykły telefon lub telefon VoIP USB
Dzwonienie za pomocą komputera z komunikatorem	Jeśli często dzwonimy, ten typ telefonowania nie jest najwygodniejszy. Docenią go jednak osoby, których znajomi już korzystają z komunikatorów internetowych i lubią bardzo długo rozmawiać – komunikatory pozwalają bowiem na zupełnie darmową rozmowę. Dodatkowo jeśli podłączymy kamerę, nasz rozmówca nie tylko będzie mógł nas usłyszeć, ale także zobaczyć. Prosta kamera internetowa to wydatek od 50 do 150 zł.	Słuchawki z mikrofonem + komunikator + dodatkowo kamera
System wdzwaniany	Ten typ systemu pozwala na tanie dzwonienie przez Internet z wykorzystaniem wyłącznie stacjonarnej linii telefonicznej. Nie trzeba mieć ani dostępu do Internetu, ani nawet komputera. System wdzwaniany oferuje większość operatorów VoIP.	Zwykły telefon

Technologia VoIP pozwala znacznie obniżyć rachunki telefoniczne. Wymaga jednak pewnych inwestycji na samym początku korzystania z dzwonienia przez Internet. Największym wydatkiem jest łącze internetowe, za pomocą którego są realizowane rozmowy VoIP. Bez dostępu do Internetu też można nieco zaoszczędzić na rozmowach, korzystając z systemów wdzwanianych VoIP. Dokładne instrukcje jak z nich korzystać znajdują się na witrynach WWW większości operatorów VoIP.

W przypadku, gdy chcemy, by telefonia internetowa była alternatywą dla tradycyjnej, musimy mieć dostęp do Internetu i to najlepiej szerokopasmowy. Dodatkowo musimy ponieść koszty odpowiedniego sprzętu. W tym wypadku cena ściśle zależy od wygody korzystania z VoIP. Gdy prowadzimy rozmowy długie ale sporadyczne, wystarczą słuchawki z mikrofonem. Jeśli jednak VoIP ma zastąpić tradycyjną linię telefoniczną, inwestycja będzie droższa, jednak wcześniej czy później zwróci się ona, i to z nawiązką.

#### 54. Pięć najczęstszych błędów przy tworzeniu haseł <sup>2</sup>

Marne hasło to jak niedomknięte drzwi - wręcz zapraszają złodziei, aby cię okradli. Aby temu zapobiec, powinieneś znać najczęstsze błędy popełniane podczas wymyślania haseł. Dowiedz się, jak dobrać optymalne hasło.

**Konto w banku internetowym**, sklepie online, skrzynka poczty elektronicznej, konto w internetowym domu aukcyjnym lub inne serwisy online - hasła są potrzebne na każdym kroku. To irytuje i nakłania do stosowania wszędzie tego samego hasła. Właśnie tak postępuje wielu internautów, popełniając niniejszym jeden z najczęstszych błędów. Jest on doskonale znany cyberprzestępcom, którzy wykorzystują go w bezlitosny sposób.

<sup>2</sup> <http://www.pcworld.pl/news/356910/Piec.najczestszych.bledow.przy.tworzeniu.hasel.html>



Abyś nie padł ich ofiarą, przygotowaliśmy zestawienie pięciu najgorszych błędów, które mogą ci się przydarzyć, gdy będziesz potrzebował nowego hasła.

Ponadto znajdziesz poniżej rady opisujące, jak tworzyć bezpieczne hasła i jak nimi zarządzać w wygodny sposób za pomocą bezpłatnego programu.

### **Błąd 1 - hasło jest zbyt krótkie, więc można je szybko złamać**

Internauci wybierają często krótkie hasła, bo są łatwiejsze do zapamiętania. Jednak większa wygoda bardzo negatywnie odbija się na bezpieczeństwie. Przykładowe obliczenie unaocznia, jak długo hasło wytrzyma atak siłowy. Takim mianem określa się procedurę, w której program usiłuje odgadnąć hasło, wypróbując po kolei wszystkie możliwe kombinacje. Przypuśćmy, że długość hasła wynosi 6 znaków i składa się ono tylko z małych liter. Oznacza to, że wchodzi w rachubę 26 znaków, co przy podanej długości hasła daje w wyniku 308 915 776 kombinacji (26 do potęgi 6). Wydaje się, że to ogromna liczba. Tymczasem nowoczesny komputer z szybkim procesorem jest w stanie złamać takie hasło w ciągu zaledwie 10 sekund!

**Zalecenie.** Bezpieczne hasło powinno składać się co najmniej z ośmiu znaków, a ponadto zawierać wielkie i małe litery. Do złamania takiego hasła za pomocą ataku siłowego potrzeba mniej więcej dwóch miesięcy. Wydłużenie hasła o choćby jeden znak i stosowanie znaków innego typu (cyfr, znaków interpunkcyjnych i innych znaków specjalnych oprócz małych i wielkich liter) wielokrotnie zwiększa czas wymagany do jego ustalenia metodą polegającą na wypróbowywaniu wszelkich możliwych kombinacji.

Jeżeli zamierzasz używać hasła za granicą, zrezygnuj z używania znaków specjalnych w hasle (przynajmniej tymczasowo) lub przynajmniej zasięgnij z góry informacji, jakimi skrótami klawiaturowymi wpisuje się je na obcojęzycznych klawiaturach.

### **Błąd 2 - hasło jest zbyt proste, więc można je odgadnąć**

Po skopiowaniu pliku języka trzeba włączyć polski interfejs. Hasło jest zbyt łatwe do odgadnięcia, gdy składa się z jednego słowa, które występuje w słowniku (dowolnego języka). Długość hasła odgrywa w tym wypadku drugoplanową rolę. Najprostszą metodą łamania haseł jest tzw. atak słownikowy. Zasada jego działania jest podobna do ataku siłowego, z tym że zamiast wszystkich możliwych kombinacji z wybranego zakresu znaków narzędzie wypróbuje kolejno wszystkie wyrazy zawarte w określonym pliku słownika. Nawet pecet o przeciętnej wydajności nie potrzebuje wiele czasu, aby przerobić cały słownik średniej objętości.

W takim pliku słownika można umieścić nie tylko zwyczajne wyrazy, lecz także listę liczb. Dlatego nie zaleca się obierać za hasło daty urodzin. Równie proste do złamania są hasła utworzone wg określonego wzorca. Unikaj więc ciągów znaków takich jak *12345* czy *qwerty*, lecz również *abcdef*.

**Przykład.** Jeden z pracowników serwisu społecznościowego Twitter chciał zabezpieczyć swój profil hasłem *happiness* (z ang. szczęście). Pewien osiemnastoletni haker przeprowadził nocą atak słownikowy na ten profil. Już następnego dnia odkrył prawidłowe hasło. A ponieważ złamał profil administratora, mógł przejąć kontrolę nad wszystkimi kontami innych użytkowników, które gromadzi Twitter. Zaatakowanie tą metodą okazało się możliwe, bo Twitter dopuszczał dowolną liczbę kolejnych prób przy nieudanym zalogowaniu. Warto zauważyć, że podobnie jest w wielu innych portalach internetowych.

**Zalecenie.** Dobre hasło nie powinno znajdować się w żadnym ze słowników, a więc być pozbawione jakiegokolwiek sensu.

### **Błąd 3 - hasło jest gdzieś zanotowane lub zapisane cyfrowo**

Dostępu do bazy chroni hasło główne - należy je dobrze zapamiętać lub zanotować i przechowywać w bezpiecznym miejscu. Nawet najlepsze hasło może w mgnieniu oka stać się bezwartościowe, gdy jest zapisane w niezaszyfrowanej postaci gdziekolwiek na twardym dysku. Wówczas może zostać podejrzane przez hakera lub złośliwy program. Niektórzy użytkownicy wysyłają wręcz swoje hasła na własny adres pocztowy, aby móc z nich korzystać, gdziekolwiek się znajdują. Inni notują swoje hasła na kartce, skąd mogą zostać przeczytane przez nieprzychylną osobę.

**Zalecenie.** Najlepiej zapamiętywać wszystkie swoje hasła. Jednak w wypadku skomplikowanych haseł okazuje się to niezwykle trudne. Gdy zechcesz je przechować w komputerze, powinieneś skorzystać z menedżera haseł, który pełni rolę swego rodzaju sejfu. Hasła są tu gromadzone

w zaszyfrowanej postaci, a więc zabezpieczone przed kradzieżą. Sam sejf jest chroniony tzw. hasłem głównym. Powinno ono być wyjątkowo bezpieczne, bo jest jedyną przeszkodą, która broni dostępu do wszystkich innych haseł. Ponadto nie powinieneś nigdzie notować swojego hasła głównego. Nie zapomnij go, bo byłoby to równie fatalne w skutkach. Wówczas straciłbyś dostęp do wszystkich swoich haseł, a nie uda ci się złamać silnego hasła głównego.

Aby bezpiecznie przechowywać swoje hasła, możesz skorzystać z bezpłatnego programu KeePass Password Safe Professional 2.10 lub KeePass Password Safe 1.17. Działa w środowiskach Windows XP, Vista i Windows 7. Aby uzyskać polską wersję interfejsu, pobierz tłumaczenie (do wersji 1.17, do [wersji 2.10](#)), po czym skopiuj zawartość archiwum ZIP do katalogu, w którym jest zainstalowana aplikacja. Następnie uruchom ją i wskaż polecenie *View / Change language*.

Jeśli brakuje ci fantazji, skorzystaj z wbudowanego generatora haseł.

#### **Błąd 4 - używanie latami tego samego hasła**

Wielu użytkowników stosuje od lat to samo hasło. Jest to bardzo ryzykowne, bo można nie zauważyć, że w międzyczasie zostało wykryte przez agresora. W najlepszym wypadku haker ma więc nieograniczony czasowo dostęp do zasobów chronionych hasłem i może np. długimi miesiącami lub wręcz latami niepostrzeżenie czytać twoją korespondencję. Wg przeprowadzonej przez nas ankiety na początku 2008 r. ponad 39 procent internautów nigdy nie zmienia swojego hasła, zaś kolejne 34 procent robi to bardzo rzadko. **Zalecenie.** Zmieniaj regularnie swoje hasła. Potrzeba do tego niezwykłej kreatywności. Znacznie lepiej użyć do tego celu generatora haseł. Narzędzie tego typu znajdziesz m.in. we wspomnianym powyżej programie KeePass Password Safe. Wystarczy utworzyć nowy wpis, a aplikacja samodzielnie opatrzy go bezpiecznym hasłem. Chcąc ujrzeć hasło w jawnej postaci, kliknij ikonę tuż obok pola z hasłem. Więcej propozycji haseł uzyskasz za pomocą kolejnych kliknięć. Warunki, które musi spełniać nowe hasło ustawisz poprzez menu *Narzędzia | Generuj hasło* (wersja 2.x) lub *Narzędzia | Generator haseł* (wersja 1.x). Powinieneś tu wybrać używanie znaków specjalnych.

#### **Błąd 5 - używanie jednego hasła do wszystkiego**

KeePass Password Safe podaje, na ile bezpieczne jest wpisywane przez ciebie hasło. Skrzynki pocztowe, system Windows, archiwa ZIP i RAR, nasza-klasa, facebook, fora internetowe, Gadu-Gadu czy ICQ - bardzo szybko zbierze ci się wiele haseł do zapamiętania. Dość popularny błąd polega na obraniu jednego hasła do wszystkich serwisów internetowych. Jest to wygodne, bo zamiast wielu wystarczy zapamiętać tylko jedno hasło. Ale gdy komuś uda się je podpatrzeć, ukraść lub złamać, odniesiesz ogromną stratę. Wówczas agresor uzyska za jednym zamachem dostęp do wszystkich serwisów internetowych, w których jesteś zarejestrowany, a być może także do twojej poczty, komunikatora i poufnych, zaszyfrowanych dokumentów. Hakerzy mają w zwyczaju wypróbować złamane hasła w innych miejscach, gdzie jest wymagane logowanie lub ich wpisywanie. **Zalecenie.** Nie powielaj haseł. Do każdego nowego zabezpieczenia dobieraj inne hasło. Aby ułatwić sobie ich zapamiętanie, przechowuj je w specjalnym menedżerze haseł, np. opisanym powyżej KeePass Password Safe.

Podsumowanie - jak wygląda hasło nie do złamania?

Wiele serwisów internetowych dopuszcza(ło) dowolną liczbę prób logowania. Twitter padł ofiarą ataku słownikowego przeprowadzonego przez 18-letniego hakera. Dobre hasło jest możliwie długie. Absolutne minimum to osiem znaków. Zawiera nie tylko małe i wielkie litery, lecz również liczby i znaki specjalne.

Unikaj haseł, które mogą występować w słownikach. Najlepiej używać hasła utworzonego za pomocą generatora haseł (np. z programu KeePass Password Safe).

Pod żadnym pozorem nie zapisuj haseł ani innych kodów dostępu w jawnej postaci w komputerze. Nie notuj ich na kartce, która może wpaść w ręce osób trzecich. Oprócz tego zmieniaj swoje hasło co kilka tygodni.

10 najgorszych haseł

Firma **McAfee** specjalizująca się w projektowaniu oprogramowania zabezpieczającego ustaliła najczęściej używane hasła w Europie. Okazało się, że w każdym hasle tkwił przynajmniej jeden błąd. W ankiecie wzięło udział około 3500 użytkowników. Na podstawie tego badania sporządzono listę 10 najgorszych haseł.

- |   |                                      |
|---|--------------------------------------|
| <b>1.</b> nazwa zwierzęcia domowego               | <b>6.</b> imię partnera/partnerki    |
| <b>2.</b> nazwa swojego hobby                     | <b>7.</b> własne imię                |
| <b>3.</b> nazwisko rodowe matki                   | <b>8.</b> ulubiona drużyna piłkarska |
| <b>4.</b> data urodzin jednego z członków rodziny | <b>9.</b> ulubiony kolor             |
| <b>5.</b> własna data urodzin                     | <b>10.</b> nazwa pierwszej szkoły    |