1 Problemy i zagrożenia

Każdy kij ma dwa końce, a każda dobra rzecz swoje ciemne strony. Jakie negatywne zjawiska wiążą się z masową komputeryzacją? Można tu wymienić kilka obaw i rzeczywistych zagrożeń: pierwszym i najwcześniej dostrzeżonym jest groźba bezrobocia, drugim zagrożenie prywatności, trzecim przestępczość komputerowa a czwartym groźba utraty ważnych danych.

Podobnie jak rewolucja przemysłowa na początku XIX wieku wzbudzała masowe protesty wśród tracących pracę rzemieślników, tak i rewolucja informatyczna końca XX wieku wzbudzała, począwszy od lat 60-tych, wielkie obawy. Przewidywano likwidację milionów miejsc pracy, eliminację wielu zawodów przez daleko posuniętą mechanizację. Okazało się coś wręcz odwrotnego: kraje najbardziej miały najniższe wskaźniki bezrobocia.

Nie można wykluczyć, że na dłuższą metę zapowiadane przez różnych futurystów bezrobocie strukturalne ujawni się, a wszelkie procesy produkcyjne w znacznej mierze będą całkowicie zautomatyzowane. Między innymi przewiduje się, że automatyzacja kontroli lotów samolotów w połowie lat 90-tych znacznie zmniejszy zapotrzebowanie na tych wysoce kwalifikowanych pracowników. Większość osób w krajach rozwiniętych pracuje już teraz w usługach a nie w rolnictwie czy produkcji. Wprowadzenie technik komputerowych stworzyło bardzo wiele miejsc pracy i nowych zawodów. Liczba różnych zawodów w latach 90-tych naszego stulecia jest czterokrotnie wyższa niż przed pięćdziesięciu laty a liczba wąskich specjalizacji, często istniejących tylko przez 10-20 lat i znikających w wyniku postępu technicznego, ciągle szybko rośnie.

Inną obawą, która okazała się płonną, jest strach przed dehumanizacją życia na skutek wprowadzania nowych technik. Skrajną formą tego strachu jest **technofobia**. Polega ona na wpadaniu w panikę przed wszystkim, co techniczne, wierze w tajemnicze złe wpływy, ,,promieniowanie" monitorów i kuchenek mikrofalowych. Pomaga w tym prasa: rzadkie wypadki spowodowane przez roboty są mocno nagłaśniane pod sensacyjnymi nagłówkami: ,,Robot zabił człowieka", podczas gdy tylko wyjątkowo duże wypadki odnotowywane są w prasie w fabrykach nie używających robotów. Wielką obawą było powstanie nowej klasy ,,wtajemniczonych" technokratów, mających dostęp do informacji i przez to kontrolujących świat. Obawy te, w znacznej mierze na skutek większego rozpowszechnienia komputerów i lepszego zrozumienia, czym są bazy danych, uległy przytłumieniu. Pozostaje jednak faktem, że wielu całkiem inteligentnych ludzi ma kłopoty z zaprogramowaniem magnetowidu tak, by automatycznie nagrał wybrany program.

Całkiem realne są natomiast obawy przed zagrożeniem prywatności. Coraz więcej firm i agencji rządowych zbiera o nas informacje. Zdarza się, że są to informacje niesprawdzone i nieprawdziwe, ale raz zapisane w bazie danych mogą nam zaszkodzić. Informacje o przyjmowanych przez nas lekach, przebytych chorobach, otrzymanych mandatach, stosunku do różnych organizacji politycznych czy religijnych, prędzej czy później mogą znaleźć się w bazie danych i wpaść w niepowołane ręce. Próby założenia krajowej bazy danych o obywatelach w Stanach Zjednoczonych doprowadziły, na skutek takich właśnie obaw, do czegoś wręcz przeciwnego, a mianowicie do uchwalenia prawo do prywatności. W wielu krajach europejskich uchwalono również takie prawo. Zabrania ono gromadzenia danych o obywatelach przez instytucje do tego niepowołane, daje prawo do wglądu do własnych akt i poprawy znajdujących się w nich nieścisłości. Wprowadzenie numerów identyfikacyjnych PESEL - wszystkie kraje zachodnie, łącznie z USA, mają również takie numery - ułatwia pracę urzędom podatkowym, ułatwia też dotarcie do informacji przechowywanych przez różne instytucje. Komputerowe bazy danych można, przy pewnym wysiłku związanym ze zdobyciem praw dostępu, przeszukiwać zdalnie, korzystając z sieci.

Innym aspektem, związanym z zagrożeniem prywatności, jest możliwość nieustannej obserwacji pracownika przez jego przełożonych. To poczucie, że ktoś nam ciągle zagląda przez ramię, jest dla wielu ludzi trudne do zniesienia. Pracownicy są zwalniani jeśli tylko wyniki ich pracy odbiegają nieco od normy. Amerykańskie telefonistki muszą załatwiać średnio 2 rozmowy na minutę, nie można więc sobie pozwolić na żarty przez telefon - komputer bez przerwy oblicza wydajność pracy.

1.1 Kiedy komputer się myli.

Fałszywe dane w bankach informacji trudno jest nieraz poprawić przez całe lata. Dotyczy to urzędów podatkowych i innych agencji rządowych - sytuacje nietypowe, dla których w programie zbierającym informację nie przewidziano odpowiedniej rubryczki, są często przez urzędników ignorowane. Autor tej książki sam stał się ofiarą takiej sytuacji - amerykański urząd podatkowy po ponad rocznym wysyłaniu ponaglenia do płacenia podatków przez urzędy lokalne, stanowe i federalne w końcu zagroził mi przysłaniem komornika - pomimo tego, że na każde pismo urzędy otrzymywały odpowiednie wyjaśnienie wraz z kopiami dokumentów, zwalniających od płacenia podatków. Dopiero spędzenie połowy dnia na rozmowach w lokalnym urzędzie podatkowym ostatecznie wyjaśniło sprawę. Innym razem konsulat amerykański stwierdził, że parę lat wcześniej nie wydano mi wizy, musiała więc być jakaś przyczyna. Przez parę dni usiłowałem przypomnieć sobie o co mogło chodzić, aż w końcu sobie przypomniałem - złożyłem wniosek o wizę, a potem z wyjazdu zrezygnowałem. Na szczęście po takich incydentach programy są doskonalone i pomyłki zdarzają się coraz rzadziej.

Trudno tu mówić o pomyłkach komputerów, chodzi raczej o błędy programistów, którzy nie przewidzieli wszystkich możliwości. Stosunkowo często pomyłki zdarzają się w systemach telefonicznych, gdyż systemy te sterowane są wyjątkowo złożonym oprogramowaniem. Czasami skutki pomyłek lub nieuwzględnienia wszystkich możliwości przez programistów mogą być tragiczne. Błędy w programach komputerowych sterujących rakietami obronnymi w czasie wojny w Zatoce Perskiej kosztowały życie kilkudziesięciu żołnierzy. W jednej z łodzi podwodnych zaciął się zamek uwalniający torpedę, pomimo tego pokładowy komputer spowodował jej wybuch i łódź zatonęła. Błąd w programie kontrolującym działanie bomby kobaltowej, niszczącej promieniowaniem gamma komórki rakowe, kosztował życie pacjenta. W 1992 roku doszło do awarii systemu kontrolującego wezwania karetek pogotowia w Londynie: program określający, która karetka jest najbliżej miejsca wezwania nie mogąc w niektórych przypadkach podjąć jednoznacznej decyzji, spychał wezwanie na koniec listy, co doprowadziło do opóźnień dochodzących do opóźnień dochodzących do pół godziny. Oceniono, że ten błąd oprogramowania kosztował życie 10-20 osób. Przykłady można by mnożyć. Kto w takich przypadkach jest odpowiedzialny? Czy należy posadzić na ławie oskarżonych programistów za nieumyślne spowodowanie zabójstwa? W przypadku karetek Londyńskich sąd stwierdził, że zgony nastąpiły z przyczyn naturalnych, nie pociągając nikogo do odpowiedzialności, jedynie jeden z dyrektorów odpowiedzialnych za wprowadzenie systemu komputerowego (zakupiono najtańszy od firmy nie mającej doświadczenia w tego typu pracy) poddał się do dymisji.

Zdając sobie sprawę z zawodności oprogramowania komputerowego, znaczna część amerykańskich programistów wypowiadała się przeciwko budowie automatycznego systemu obrony, znanego pod kryptonimem ,,wojny gwiezdne". Byłby to system tak złożony, że prędzej czy później błędy w oprogramowaniu mogłyby doprowadzić do globalnej katastrofy. Wiadomo, że systemy wczesnego ostrzegania, stosowane od lat przez armię amerykańską, nieraz podnosiły fałszywy alarm, związany z pojawieniem się stada ptaków lub wschodem Księżyca.

Człowiek myli się w sposób przypadkowy i dlatego bardzo trudno jest powtórzyć dokładnie taką samą sytuację. Większość błędów w programach komputerowych daje się łatwo wykryć, gdyż błędne wyniki powtarzają się regularnie. Bardzo skomplikowane programy nie dają się jednak przetestować tak, by uwzględniły wszystkie możliwe sytuacje, stąd firmy komputerowe wypuszczają najpierw w celach testowych wersje programów zwane ,,beta", a po usunięciu niedoskonałości jeszcze wersję ,,alfa", testowaną przez wybranych użytkowników, przed ostatecznym wprowadzeniem programu do sprzedaży. Programy używane na komputerach osobistych przechodzą nie tylko te dwie fazy testowania, ale sprawdzane są w praktyce przez miliony użytkowników, którzy znajdują w nich drobne błędy, usuwane w wersjach oznaczanych kolejnymi numerami, np. po DOS 4.0 wprowadzono DOS 4.01. Żaden inny rynek komputerów nie ma tak wielu użytkowników, stąd szansa na znalezienie błędu w oprogramowaniu używanym na komputerach centralnych czy w oprogramowaniu

specjalistycznym, zwykle dużo bardziej złożonym niż proste programy powszechnego użytku, jest dużo większa niż w przypadku znanych firm sprzedających miliony swoich programów na rynku komputerów osobistych. Projekty ścisłej weryfikacji poprawności działania programów przy pomocy metod matematycznych, wysuwane przez znanych informatyków, dalekie są jeszcze od zastosowań praktycznych i nie wiadomo, czy takie metody kiedykolwiek będą użyteczne.

Komputery to dobre kozły ofiarne - coraz częściej swoje błędy redaktorzy gazet zwalają na komputery. Zamiast przeprosić za pomyłkę sprostowania noszą tytuł: „Komputer zjadł literkę".

1.2 Przestępstwa komputerowe

Nie ma wątpliwości, że będziemy polegać w coraz większym stopniu na komputerowej łączności, przepływie pieniędzy i gromadzeniu informacji. Stwarza to wielkie zagrożenia zdalnego ,,podglądania" wszystkiego, co robimy, ciągłej obserwacji naszej pracy i wykradania jej rezultatów. Najbardziej zagrożone są oczywiście instytucje finansowe: liczba przestępstw komputerowych może nie wydawać się tak wielka, gdyż banki nie chwalą się słabościami swoich systemów zabezpieczeń, ale sumy, skradzione dzięki przestępstwom komputerowym znacznie przekraczają ,,dochody" z napadów z bronią w ręku. Poważne niebezpieczeństwo grozi również firmom telekomunikacyjnym: rozliczenie kosztów połączeń dokonuje system komputerowy, więc jeśli uda się do niego włączyć i trochę pozmieniać mu dane można przestać płacić rachunki lub obciążać nimi konto jakiejś dużej firmy. Straty z tego tytułu szacowane są w USA na miliardy dolarów, stąd obsesja na punkcie bezpieczeństwa nowo wprowadzanych systemów.

Z drugiej strony globalne sieci komputerowe są potężną bronią w walce z przestępczością - w Stanach Zjednoczonych już od wielu lat nawet w odludnych wioskach sklepy i motele przyłączone są liniami telefonicznymi do baz danych instytucji finansowych i w ciągu sekund mogą sprawdzić ważność kart kredytowych.

Chociaż żerowanie na naiwności laików nie zawsze ma znamiona przestępstwa, z pewnością jest postępowaniem nieetycznym. W łagodnej formie sprowadza się to do oferowania trywialnie prostych programików, które każdy rozgarnięty informatyk może napisać w parę godziny za setki tysięcy złotych (różne doróbki polskich liter, druk lustrzany). Często są to programy rozpowszechniane jako shareware lub rozdawane za darmo. W cięższych przypadkach jest to wciskanie drogich komputerów i jeszcze droższych programów do prostych zastosowań.

Najpowszechniejszym jednak komputerowym przestępstwem jest piractwo **komputerowe**, szerzące się dramatyczne we wszystkich krajach świata. Nawet w krajach

o dużej tradycji ochrony praw autorskich nie zdarza się prawie, by za nielegalne skopiowanie lub używanie oprogramowania sąd ukarał indywidualną osobę. Zdarza się natomiast nakładanie wysokich kar na duże firmy używające nielegalnie oprogramowania czy na osoby handlujące kradzionym oprogramowaniem. Jeszcze częściej zdarzają się obecnie kontrole w sieciach komputerowych i BBSach, łącznie z konfiskatą sprzętu i dokumentacji. Niektórzy operatorzy BBSów umieszczają w nich oprogramowanie chronione prawami autorskimi, umożliwiając do niego dostęp wszystkim subskrybentom. Zabezpieczenia w postaci kluczy sprzętowych, jedyne naprawdę skuteczne zabezpieczenia oprogramowania działającego na komputerach osobistych, nie są zbyt popularne. Fachowcy starają się unikać tego typu oprogramowania, jeśli ma się kilka programów chronionych kluczami sprzętowymi, staje się to bardzo uciążliwe.

Szacowane w 1992 roku straty z powodu piractwa komputerowego wyniosły ponad 2 miliardy dolarów US, przy całkowitej sprzedaży 6.6 mld $. Szacowane straty amerykańskie w Polsce miały wynieść 100 mln $. Największe straty z tego tytułu (w milionach dolarów w 1992 roku) amerykanie ponieśli w następujących krajach: Tajwanie (585), Hiszpanii (336), Korei Północnej (315), Włoszech (238), Rosji i Polsce (po 100 mln $). Krajom tym grożono okresowym cofnięciem ulg celnych do czasu wprowadzenia odpowiednich przepisów o ochronie praw autorskich. Nie wiadomo jednak, w jaki sposób oszacowano te straty. Trudno przecież założyć, że każdy użytkownik, który używa drogiego oprogramowania amerykańskiego kupi je, jeśli tylko będą obowiązywać odpowiednie przepisy. Można się natomiast spodziewać, że taki użytkownik kupi tanie, lokalnie produkowane oprogramowanie, a więc wprowadzenie przepisów o ochronie praw autorskich wpłynie korzystnie na lokalny przemysł oprogramowania. Największe straty ponoszą producenci oprogramowania z powodu nielegalnego używania ich produktów przez organizacje i przedsiębiorstwa, a te czują się zmuszone do legalizacji oprogramowania dopiero po wydaniu odpowiednich przepisów prawnych.

Piractwo komputerowe ograniczone jest do komputerów osobistych i domowych. W systemach wielodostępnych (np. w Unixie) uruchomienie programu wymaga jego rejestracji w systemie przy pomocy programu zwanego Menedżerem Licencji (License Manager). Oszukanie tego programu nie jest proste, stąd nielegalne używanie oprogramowania raczej nie wchodzi w grę - każda stacja ma swój numer i kupujący otrzymuje licencję na konkretny komputer. Ogranicza się również liczbę użytkowników, mogących korzystać jednocześnie z programu dostępnego przez sieci komputerowe.

Coraz częściej sprzedaje się oprogramowanie na CD-ROMach. Ponieważ na jednym CD-ROMie zmieścić można bardzo wiele różnych programów, grafiki, krojów czcionek itp. producenci wpadli na ciekawy pomysł - na dysku znajduje się od razu bardzo bogate oprogramowanie, ale jego uaktywnienie wymaga znajomości specjalnego hasła. Kupujący dostaje więc kolejne hasła pozwalające na korzystanie z tych programów, które już ma na dysku, ale za które zdecydował się zapłacić w późniejszym terminie.

Wprowadzenie CD-ROMów spowodowało rozwój innego negatywnego zjawiska - **pornografii komputerowej**. Proste obrazki pornograficzne można było zakupić od dawna na dyskietkach, dopiero jednak możliwości przechowywania dużej liczby zdjęć i fragmentów animowanych na CD-ROMach zrobiły z komputerów atrakcyjne medium do rozpowszechniania pornografii. Pornografia i prostytucja komputerowa rozpowszechnia się szybko u naszych zachodnich sąsiadów dzięki sieciom komputerowym, szczególnie przez szybkie połączenia sieciami ISDN w ramach systemu terminali telefonicznych Btx. W sex-shopach sprzedaje się coraz więcej komputerowo sterowanych przystawek, w tym również do wirtualnej rzeczywistości. Szczególnie trudnym problemem jest filtrowanie informacji pochodzących z sieci globalnych. Serwery WWW przechowujące rysunki i teksty pornograficzne trudno będzie ocenzurować i istnieje realne niebezpieczeństwo, że wędrujące po cyberprzestrzeni dzieci natkną się na tego typu materiały. Rozwiązaniem jest instalacja oprogramowania blokującego dostęp do pewnych węzłów sieci, np. oprogramowania Cyber Patrol (Microsystem Software), osiągalnego pod adresem http://www.microsys.com lub innego oprogramowania wykrywającego nieprzyzwoite słownictwo i blokujące dostęp do zawierających je stron. Jeśli jednak w pliku graficznym nazwa wygląda niewinne program sam nie zgadnie, jaka jest treść zapisanego w nim obrazu. Dlatego niektóre programy (np. Cybersitter) sprzedawane są z bazą danych, zawierających wykaz podejrzanych węzłów Internetu. Chociaż pornografia komputerowa to bez wątpienia poważny problem używając Internetu od 10 lat nigdy nie natknąłem się na pornograficzne treści - widać ich sam nie szukałem.

Poważnym problem stają się również włamania do sieci komputerowych. Włamywacz, nazywany czasami hackerem, potrafi dokonać bezsensownych zniszczeń w systemie komputerowym lub skopiować ważne dane. Włamywanie do systemów komputerowych podlega w większości krajów (również w Polsce) karze więzienia, niektórym ludziom trudno się jednak przed tym powstrzymać. Włamują się na cudze konta, włamują się również do instytucji wojskowych. Najpilniej strzeżone tajemnice wojskowe znajdują się podobno w systemach komputerowych, które nie są fizycznie podłączone do sieci ani do modemu a osoby mające do nich dostęp są odpowiednio sprawdzane. Wprowadzenie w kwietniu 1995 roku narzędzi o nazwie Satan (Security Administrator Tool for Analyzing Networks), pomagającym administratorom sieci dołączonych do Internetu wykrywać słabe punkty w ich zabezpieczeniach, ułatwiło również przestępcom zdobycie informacji o sposobach włamań. Satan miał zmusić administratorów sieci do wysiłku zmierzającego do poprawy bezpieczeństwa, ale nie każda domena sieci ma administratora, który jest na tyle doświadczony i ma na tyle dużo czasu, by poświęcać go kwestiom bezpieczeństwa. Szczegółowe informacje na temat Satana znaleźć można w węźle WWW http://www.ziff.com~pcmag

Istnieje publicznie dostępne oprogramowanie pomagające zgadywać hasła w sieciach komputerowych. Wiele systemów ma bardzo proste hasła lub pozwala dołączyć się przez sieć bez żadnego hasła. Otrzymałem kiedyś ostrzeżenie od administratora systemu z żądaniem zmiany hasła, gdyż jego program łatwo je znalazł. Proste hasło **duchduch**, którego wówczas użyłem w sieci Internetu, odkryć potrafi większość programów do

łamania zabezpieczeń. Używanie powszechnie znanych dat lub swojej daty urodzin jest również niebezpieczne. Szczególnie niebezpieczne są komputery osobiste używane jako terminale. Łatwo jest na nich założyć program rezydentny przechwytujący wszystkie polecenia wpisane przez niczego nie podejrzewającego użytkownika, łącznie z jego hasłem i wszystkimi prywatnymi wiadomościami. Prawdziwym wyzwaniem dla hackerów są jednak dobrze zabezpieczone systemy wojskowe lub bankowe - ocenia się, że system komputerowy Pentagonu atakowany jest kilkaset razy dziennie.

Próbę zbudowania systemu umożliwiającego elektroniczne transakcje bankowe przyrównuje się czasami do próby zrobienia banku bez ścian. W 1995 roku rosyjski hacker z Petersburga włamał się do amerykańskiej sieci bankowej Citycorp i zanim został wykryty i aresztowany zdołał przelać kilkanaście milionów dolarów na rachunki swoich przyjaciół. Nic dziwnego, że elektroniczne usługi bankowe rozwijają się powoli. Proponowano różne rozwiązania, np. układ elektroniczny do szyfrowania informacji o nazwie Clipper, do którego klucze wzorcowe mieliby pracownicy rządu, na co oczywiście niewiele osób skłonnych było się zgodzić. Rozwiązaniem może być opracowany w 1995 roku przez AT&T Bell Laboratories i firmę VLSI Technology układ scalony IVES (**I**nformation **V**ending **E**ncryption **S**ystem, czyli system kodowania przy sprzedawaniu informacji). Jego twórcy twierdzą, że jest on absolutnie bezpieczny i nawet sam producent nie zna klucza do odkodowania informacji. Każdy układ scalony IVES wykorzystuje 32-bitowy mikroprocesor typu RISC i korzysta z niepowtarzalnego klucza do kodowania i dekodowania informacji. Opracowano również technologię cyfrowych podpisów. Polega ona na dołączeniu fragmentu zaszyfrowanego tekstu do przesyłanej wiadomości. Przy odbiorze można sprawdzić, czy wiadomość nie została po drodze zmieniona i ustalić tożsamość nadawcy. Jest to możliwe dzięki zaawansowanym technikom kryptograficznym, opartym na publicznie dostępnym kluczu.

Systemy operacyjne używane w zastosowaniach wymagających dużego stopnia bezpieczeństwa (systemy bankowe, wojskowe, administracji rządowej) muszą przejść liczne testy, które wykonuje amerykańskie Krajowe Centrum Bezpieczeństwa Komputerowego (National Computer Security Center) by otrzymać certyfikat określający klasę bezpieczeństwa. Klasą bezpieczeństwa określaną jako C2 wyróżniono system Unix oraz Windows NT, również system Novell NetWare stara się o taki certyfikat.

Z drugiej strony nie należy zapominać, że komputery bardzo przyczyniają się do zwiększenia bezpieczeństwa w wielu aspektach: dzięki komputerowej łączności, bazach danych o przestępstwach, współdziałaniu policji i służb celnych. Systemy analizy mowy podsłuchują telefony Komputerowe systemy kontroli pracowników pozwalają śledzić ruch i kontrolować dostęp poszczególnych osób do pomieszczeń i urządzeń w elektrowniach atomowych i zakładach wojskowych. Systemy zabezpieczeń rozpoznają człowieka na podstawie trójwymiarowych pomiarów biometrycznych dłoni, odcisków palców, zdjęcia twarzy w podczerwieni, obrazu dna oka lub brzmienia głosu. Komputery czuwają nad bezpieczeństwem lotu, czuwają w nocy nad pacjentami w szpitalu, pomagają śledzić przestępców i utrudniają życie terrorystom.

1.3 Wirusy komputerowe

Od paru lat użytkowników komputerów osobistych nękają komputerowe wirusy. Niestety, od czasu do czasu mniej znane firmy produkujące oprogramowanie ,,przepuszczą" jakiegoś wirusa w swoim produkcie! Najczęstszym źródłem wirusów są jednak nielegalne kopie oprogramowania. Zdarza się również, że kupowane w dobrej, wierze po wyjątkowo korzystnej cenie, programy okazują się nielegalnymi kopiami cieszącymi się niezbyt dobrym zdrowiem ... By się przed tym ustrzec znane firmy komputerowe umieszczają na dokumentacji swoich programów trudne do podrobienia znaczki holograficzne. Duże, wielodostępne systemy również nie są odporne na działanie wirusów, i choć ich ataki zdarzają się w tych systemach rzadziej konsekwencje są znacznie poważniejsze, gdyż wpływają na wielu użytkowników. Na dużych systemach prawie nigdy nie instaluje się nieznanych programów, stąd typowy sposób ,,zarażania się", przez wymianę programów, nie wchodzi raczej w grę.

Co to są owe wirusy? Są to niewielkie programy, o długości od kilkudziesięciu (!) do kilku tysięcy bajtów, które dołączają się do programów systemowych, użytkowych, instalują się na dyskietkach i w obszarach systemowych dysków twardych. Przy wywoływaniu zarażonego programu albo w trakcie uruchamiania komputera (przy ładowaniu systemu operacyjnego) wirusy rozmnażają się i dają o sobie znać.

Rozmnażając się, wirusy powielają swój program, usiłując umieścić go w różnych miejscach systemu komputerowego, zależnie od typu wirusa. Najczęściej przyklejają się do programów wykonywalnych lub programów systemowych, np. w systemie MS-DOS do programów typu EXE lub COM, nakładek do tych programów o rozszerzeniach OVL lub BIN, plików systemowych typu SYS, modułów systemu operacyjnego (COMMAND.COM, IBMBIO.COM, IBMDOS.COM), oraz bibliotek programów dołączanych do tworzonych przez użytkownika programów. Poza tym wirusy chowają się chętnie w tablicy partycji dysku stałego, w sektorze początkowym (boot sector) dysku lub dyskietki, dodatkowych ścieżkach na dyskietce, potrafią również schować się w sektorach oznaczonych jako uszkodzone. Zdarza się czasami (choć bardzo rzadko), że fragmenty programu umieszczone są w plikach o innych rozszerzeniach, ale jeśli wiemy, że dany plik jest plikiem tekstowym lub innym plikiem nie zawierającym wykonywalnego programu, to wirus nie może się w nim zagnieździć (może go za to zniszczyć.) Niektóre wirusy nic innego poza mnożeniem się nie robią. Są to łagodne, mniej szkodliwe szczepy, których stosunkowo łatwo jest się pozbyć. Czasami zauważamy brak miejsca na dysku czy dyskietce lub spowolnienie działania systemu, będące wynikiem dużej liczby kopii łagodnego wirusa, żyjącego sobie spokojnie w naszym systemie.

Niestety, znaczna część wirusów jest złośliwa. Odczekują jakiś czas, rozmnażając się w systemie, a gdy nadchodzi określona data, np. piątek 13 lub urodziny Michała Anioła, pokazują swoje kły. Najczęściej atakują dyski, niszcząc obszary systemowe, co praktycznie uniemożliwia odtworzenie zawartych na nim plików (pliki tekstowe daje się odzyskać składając je sektor po sektorze, ale jest to bardzo czasochłonna praca). Najbardziej złośliwe wirusy próbują sformatować cały dysk lub jego część, niszcząc nieodwracalnie całą zawartą na nim informację. Mogą też zmienić informację o konfiguracji systemu komputerowego, uniemożliwiając rozpoznawanie dysku (nie dotyczy to komputerów klasy XT, gdyż nie posiadają one bateryjnie podtrzymywanej informacji o konfiguracji, przechowywanej w obwodzie scalonym typu CMOS).

Niektóre wirusy ograniczają się do wyświetlania mniej lub bardziej dowcipnych napisów na ekranie komputera lub zagrania jakiejś melodyjki. Mogą też zniekształcać informację na ekranie, wymazywać literki a nawet selektywnie przestawiać cyfry w wyświetlanych na ekranie liczbach! Możliwa jest też próba fizycznego uszkodzenia sprzętu: drukarki, monitora czy napędu dysków twardych i dyskietek.

Istnieją specjalne rodzaje wirusów, znane pod nazwą ,,Koń Trojański". Są to programy wykonujące jakieś użyteczne zadania - na przykład udające, że poszukują i niszczą wirusy - jednocześnie niszczą pliki lub strukturę dysku.

Pierwsze wirusy pojawiły się przy końcu lat 80-tych. Od tego czasu programiści zrobili duży postęp i na początku 1992 roku istniało już około 80 różnych typów wirusów, posiadających prawie tysiąc odmian. Znaczna część pojawiających się w Europie wirusów posiadających prawie tysiąc odmian. Znaczna część pojawiających się w Europie wirusów pochodzi z Bułgarii, ale w każdym kraju zdarzają się programiści, gotowi zmarnować parę dni pracy, by całkowicie bezinteresownie siać na świecie zniszczenia. W Anglii powstało towarzystwo ,,szczególnie okrutnych wirusów", stawiające sobie za cel produkcję i rozpowszechnianie takich wirusów, założenie biuletynu takich wirusów i utrudniane działalności firmom telekomunikacyjnym przez fałszywe obciążanie kont abonentów telefonicznych. Na szczęście policji udało się aresztować 6 członków założycieli tego towarzystwa, pomimo tego, iż pierwszym punktem w ich deklaracji programowej było unikanie Scotland Yardu. Twórcy wirusów nie zdają sobie nawet sprawy z tego, że mogą być oskarżeni o ... morderstwo! Zdarzały się bowiem przypadki uszkodzenia przez wirusy dysków komputerów, na których w szpitalach przechowuje się dane o pacjentach. wymazanie informacji o reakcjach alergicznych na pewne leki może zakończyć się fatalną pomyłką. Żadna szanująca się firma komputerowa nie przyjmie do pracy osoby podejrzanej o tworzenie wirusów. Niektóre firmy europejskie i amerykańskie dokładnie sprawdzają kandydatów na pracowników poszukując śladów ich powiązań ze środowiskami tworzącymi wirusy a nazwiska takich osób trafiają na listy podejrzanych. Zabawa z lat młodzieńczych może przekreślić człowiekowi karierę na całe życie. Czy nie lepiej bawić się w sztuczne życie, tworzenie inteligentnych, rozmanażających się i pożytecznych programów niż bezmyślnie siać zniszczenie?

Jak chronić się przed wirusami?

Istnieje kilka metod walki z wirusami. Najważniejszą rzeczą jest unikanie kopiowania programów z niesprawdzonych źródeł. Starsze wirusy dawały się łatwo wykryć zmieniając np. długość programów systemowych. Obecnie takie proste wirusy już prawie wyginęły a wirusy nie tylko nie dają o sobie znać, ale potrafią być niewidoczne dla programów podglądających pliki na dysku! Jest kilka rodzajów programów antywirusowych.

Blokady. Są to programy dołączane do systemu operacyjnego i sprawdzające każdy uruchamiany na komputerze program. Najczęściej są to programy czuwające (TSR). Jeśli wykryją coś podejrzanego zatrzymują działanie programu. Można kupić specjalne karty rozszerzające, wspierające działanie programów blokujących. Specjalną wersją programów blokujących są szczepionki (vaccines), dołączające się do wybranych przez użytkownika programów. Po szczepieniu same sprawdzają w momencie ich uruchamiania, czy nie zostały zarażone wirusem.

Do wad programów czuwających należy: spowolnienie pracy komputera, zmniejszenie dostępnej dla użytkownika pamięci operacyjnej, konieczność podjęcia decyzji - co zrobić z wykrytym wirusem? Właściwa decyzja może wymagać pewnych wiadomości o samym wirusie. Poza tym programy te nie są w 100% pewne, gdyż wirusy, które uaktywniają się przed wywołaniem systemu operacyjnego (np. ukrywające się w tablicy partycji dysku lub ścieżce startowej) mogą nie być zauważane przez programy blokujące. Najnowsze typy wirusów potrafią całkowicie ominąć funkcje systemowe i dobrać się do sektorów dysku bezpośrednio.

Nową koncepcją jest wykrywanie wirusów dzięki analizie struktury systemów operacyjnych a nie znajomości budowy konkretnych wirusów. Dzięki temu można wykrywać wirusy jeszcze nie napisane. Instalacja takiego programu wymaga pewności, że komputer w momencie jego instalacji wolny jest od wirusów.

Strzegące. Programy takie obliczają różne parametry (tzw. sumy kontrolne) wszystkich możliwych do zarażenia programów na dysku i zapisują je w pliku. Dzięki temu można sprawdzić, czy uruchamiany program nie został zmieniony. Niestety, nie można się w ten sposób wirusa pozbyć. Doświadczeni użytkownicy potrafią się posłużyć programami narzędziowymi i samemu usunąć wirus, jest to jednak pracochłonne. Drugą wadą jest powolne działanie tego typu programów przy sprawdzaniu całego dysku.

Polujące. Są to programy wykrywające konkretne typy wirusów. Potrafią nie tylko wykrywać, ale również usuwać wirusy z systemu bez niszczenia zarażonych programów. Na ogół działają dość szybko. Wadą tego typu rozwiązania jest stosunkowo częste pojawianie się nowych wirusów, stąd trzeba takie programy ciągle uaktualniać. Niektóre

programy próbują wykrywać również ,,podejrzane" fragmenty kodu, nie jest to jednak metoda pewna: twórcy wirusów są pomysłowi i wymyślają coraz nowsze typy, poza tym ,,przeczulone" programy antywirusowe często wywołują niepotrzebny alarm.

W Polsce jednym z bardziej znanych i dobrych programów antywirusowych jest program Mks-Vir, którego autorem jest Marek Sell. Jest to szybko działający program wykrywający i usuwający wirusy, aktualizowany co miesiąc. Jego główną wadą jest stosunkowo wysoka cena. Wersja demonstracyjna, również aktualizowana co miesiąc, rozpowszechniana jest bezpłatnie i potrafi wirusy wykrywać, ale ich nie usuwa. Innym, szybko rozwijającym się, polskim programem antywirusowym, jest Doctor KK, nie tylko wykrywający wirusy, ale też szczepiący programy, by uniknąć ich zarażenia i blokujący próby zagnieżdżenia się wirusów w pamięci czy na dysku komputera. Inny polski program antywirusowy, który doczekał się już wielu wersji to V_Find. Umożliwia on profilaktykę, wyszukiwanie i usuwanie wirusów. Ponieważ liczba wirusów jest bardzo duża, programy te nie zawsze dobrze sobie radzą z wykrywaniem a zwłaszcza usuwaniem rozpoznanych wirusów.

Istnieją również dobre programy antywirusowe rozpowszechniane jako shareware, np. programy SCAN firmy McAfee czy Fprot rozsyłany siecią komputerową przez firmę z Islandii. Nie należy się obawiać o ich jakość - w testach wypadają nie gorzej niż programy renomowanych firm.

Ryzyko zarażenia można również zmniejszyć samemu. Warto jest zrobić sobie kopie plików systemowych na dyskietkę lub drugi dysk. Programy użytkowe, takie jak Norton Utilities, tworzą ,,dyskietki ratunkowe" (rescue diskettes), pozwalające odtworzyć pliki systemowe w przypadku ich uszkodzenia. Jeśli nie dysponujemy takim programem warto przynajmniej skopiować procesor poleceń (COMMAND.COM) do osobnej kartoteki lub na inny dysk. Pod ręką należy zawsze mieć zabezpieczoną przed zapisem dyskietkę sformatowaną tak, by znalazły się na niej pliki systemowe (w systemie MS-DOS jest to IO.SYS, MSDOS.sYS, COMMAND.COM oraz DBLSPACE.BIN jeśli używamy programu DoubleSpace do kompresji dysku). Warto mieć taką dyskietkę niezależnie od zagrożenia wirusami, np. w przypadku awarii dysku.

Najlepszym lekarstwem na wirusy może być jednak zabezpieczenie sprzętowe. Firma JAS Technologies opracowała kartę **Virustrap,** którą zamierza produkować Texas Instruments. Karta uruchamia się jeszcze zanim zacznie pracować system operacyjny, przechwytując próby zmian w obszarach systemowych, kontrolując pliki na twardym dysku i zabezpieczając wszystkie pliki wykonywalne. Podobne karty zamierzało wprowadzić na rynek w 1993 roku kilka innych firm.

Wirusy już spowodowały ogromne straty ale najgorsze może jeszcze być przed nami. Powstała nowa generacja przyjacielskich (!) narzędzi do tworzenia wirusów, dostępnych w publicznych archiwach Internetu (nie podaję tu ich nazw, gdyż byłaby to zachęta do niebezpiecznej zabawy). Dysponując takimi programami można całkiem przypadkiem

wyprodukować i uwolnić groźnego wirusa, który zniszczy nie tylko nasze dane, ale może zdążyć się przenieść na inne komputery. Połączenie wszystkich komputerów w jedną globalną sieć komputerową stwarza ogromne zagrożenie szybkiego rozpowszechniania się groźnych wirusów po świecie.

1.4 Inne problemy

Komputeryzacja przynieść może wiele korzyści, ale też może być przyczyną poważnych strat. Chociaż korzyści ze stosowania komputerów są oczywiste niewłaściwy wybór standardu, dostawcy, sprzętu, oprogramowania lub szkolenia pracowników może w przyszłości narazić firmę na poważne koszty.

Przykładów trudności tego rodzaju znaleźć można wiele. Biblioteki wprowadzające nietypowe systemy zmuszone były do bardzo kosztownej zmiany formatów baz danych i oprogramowania nimi zarządzającego. Niektóre amerykańskie redakcje czasopism, używające wyspecjalizowanych systemów zamkniętych, czyli nie współpracujących z produktami innych producentów, są z nich bardzo niezadowolone a przejście na nowe systemy bez przerw w pracy jest bardzo trudne. Zbytnia wiara w możliwości uporządkowania bałaganu czy rozwiązania źle postawionych problemów dzięki wprowadzeniu metod komputerowych może narobić wiele szkód. Z badań statystycznych w krajach rozwiniętych wynika, że zaledwie 5% dużych systemów informatycznych wdrożono zgodnie z planem czyli w określonym czasie, trzymając się kosztorysu i oddając gotowy system spełniający wymagania użytkownika. Ponad połowa systemów nie została w ogóle ukończona lub też nie została w ogóle ukończona lub też nie została zaakceptowana przez użytkowników.

Największym problemem jest często precyzyjne określenie, czego użytkownik od systemu oczekuje. Jest to szczególnie istotne w warunkach polskich, gdzie brak jest jeszcze dobrze wypracowanych metod zarządzania, stosowanych np. przez firmy amerykańskie. Moda na komputeryzację wprowadzaną bez zrozumienia, do czego ma ona służyć, jedynie w oparciu o przekonanie, że nowoczesne metody muszą polepszyć wyniki, prowadzi jedynie do rozczarowania. Większość projektów powstających w naszych warunkach, gdzie niewiele jest jeszcze firm, które odmówią wykonania zamówienia widząc, że nie da się go dobrze zrealizować, powstaje w sposób chaotyczny, metodą prób i błędów. Jest to w istocie dofinansowywanie przez firmy zlecające procesu przyuczania do zawodu informatyków. Pęd do nowoczesności, utożsamianej z komputerami i sieciami komputerowymi, góruje nad trzeźwą oceną korzyści, jakie daje wprowadzanie nowych technologii.

Dodatkowym problemem jest brak odpowiednich programów studiów w tej dziedzinie - informatyka uniwersytecka opiera się najczęściej na kadrze byłych matematyków,

nastawionych do swojej dziedziny bardzo teoretycznie i zaniedbujących takie zagadnienia, jak praca nad dużymi projektami. W tej dziedzinie, podobnie jak i w medycynie, teoria ma niestety rzadko zastosowanie w praktyce, liczy się przede wszystkim doświadczenie. Nieliczne bardzo profesjonalne firmy zachodnie, które pojawiły się na naszym rynku, żądają za swoje usługi niebotycznych honorariów.

Żaden producent oprogramowania nie daje na nie pełnej gwarancji, w szczególności nie odpowiada za szkody, które może wyrządzić jego stosowanie. Czy te problemy wynikają z niedojrzałości technologii informatycznych, w szczególności inżynierii oprogramowania, czy jest to nieodłączna cecha zadań o wysokim stopniu złożoności? Nie można porównywać problemów związanych z rozwijaniem złożonych systemów informatycznych z projektowaniem budowy urządzeń mechanicznych, np. mostu. Liczba możliwych sytuacji, związanych z konfiguracją sprzętu, systemem operacyjnym, współpracą z innymi programami i stanem wewnętrznym danego programu, rośnie bowiem bardzo szybko wraz z jego złożonością, osiągając dla dużych systemów niemal nieskończone wartości. Projektowanie takich systemów jest tak trudne, że oceny dotyczące kosztów i czasu trwania pracy nad programem niewiele mają wspólnego z rzeczywistością - średni błąd wynosi tu 400%!

Informatycy zauważyli te problemy już w latach siedemdziesiątych i jednym ze sposobów ich zmniejszenia jest wprowadzenie nowych, bezpieczniejszych technik oprogramowania, takich jak programowanie strukturalne i programowanie zorientowane obiektowo. Rozwinęła się również inżynieria oprogramowania (**software engineering**) oraz narzędzia **CASE** wspomagające zastosowanie tych metod w praktyce. Metody te są bardzo przydatne szczególnie w przypadku pracy zespołowej. Analiza wstępna projektu metodami inżynierii oprogramowania jest jednak sama w sobie bardzo żmudna i kosztowna. Wstępny projekt systemu informatycznego przedstawiony zostaje w postaci diagramu, który jest zrozumiały dla fachowców firmy zamawiającej oprogramowanie. Jednym z największych informatycznych projektów rządowych w Polsce jest system opracowywany dla PKP, tworzony właśnie w oparciu o narzędzia CASE.

Wielkim zagrożeniem dla dalszych możliwości rozwoju oprogramowania jest patentowanie prostych idei i technik programowania. Do końca 1992 roku w USA przyznano już 9000 patentów na oprogramowanie w takich dziedzinach jak systemy operacyjne, przetwarzanie obrazu, grafika. Liczba przyznawanych patentów rośnie coraz szybciej, z powodu obowiązujących przepisów często dla uzasadnienia przyznawanych patentów dodaje się jakieś elementy sprzętowe. Każda firma, której uda się wylansować jakieś popularne oprogramowanie, może liczyć się z zaskarżeniem przez potentatów przemysłu komputerowego (12% wszystkich licencji ma IBM) o to, że nie płacąc licencji używa jakiejś techniki, która została opatentowana. Nie tylko podraża to koszty oprogramowania, ale może doprowadzić do monopolizacji tego rynku.

Typowym przykładem problemów z patentowaniem oprogramowania jest historia **C**ompuServe **I**nformation **S**ervice (CIS), firmy amerykańskiej udostępniającej informację

w sieciach komputerowych CompuServe. Przy końcu grudnia 1994 roku CIS zażądała, by w ciągu 12 dni programiści wyrazili zgodę na płacenie tantiem za używanie opracowanego przez CIS formatu plików graficznych GIF. Jest to format grafiki rastrowej szczególnie często wykorzystywany w sieciach komputerowych ze względu na efektywną metodę wewnętrznej kompresji obrazu. Format ten został opracowany przez CIS w 1987 roku i szeroko reklamowany jako standard do kompresji plików zawierających grafikę z 256 kolorami. Przez całe lata firma CIS nic nie wspominała o tantiemach. Okazało się, że kompresja obrazu zastosowana w plikach GIF narusza patent firmy Unisys z 1985 roku na algorytm kompresji danych znany jako LZW. W rezultacie CIS musiała zapłacić Unisysowi 125.000 dolarów za licencję i zaczęła grozić twórcom oprogramowania wykorzystującym standard GIF procesami sądowymi. W Netlandii zawrzało, nikt nie chciał się zgodzić na płacenie tantiem a sprawę komentowały szeroko amerykańskie gazety. W rezultacie masowej akcji protestacyjnej koordynowanej poprzez Internet Unisys i CIS wycofały się ze swoich żądań.

Do jakich absurdów mogą doprowadzić patenty na oprogramowanie pokazała firma Compton, zastrzegając sobie prawa na zastosowania multimedialne. Praktycznie rzecz biorąc patent obejmował wszystko, co się na ekranie może poruszać. Patent został przyznany i po jakimś czasie unieważniony. Wszystkie większe firmy komputerowe są uwikłane w rozliczne procesy, skarżąc siebie nawzajem. Na całym zamieszaniu zarabiają przede wszystkim prawnicy a traci przemysł komputerowy i użytkownicy programów.

1.5 Komputerowy terroryzm ?

Uzależnienie od systemów i sieci komputerowych może się stać niebezpieczne. Możliwość docierania do dowolnych miejsc na świecie poprzez komputerowe sieci powoduje potencjalnie wielkie niebezpieczeństwo. Krążą plotki, że w czasie wojny w Zatoce Perskiej grupa hakerów z Holandii proponowała Saddamowi Husejnowi zniszczenie amerykańskiej sieci informacyjnej zaledwie za milion dolarów. Przed hakerami można się jakoś zabezpieczyć, ale prędzej czy później pojawi się nowa generacja wirusów sieciowych takich jak „bomby logiczne", wprowadzone do systemów i spoczywające w uśpieniu aż do momentu nadejścia rozkazu. Takie wirusy wbudować można w mikroprocesory i doprowadzić do umieszczenia ich w sprzęcie wojskowym przeciwnika.

Najbardziej niebezpieczne są bomby elektromagnetyczne - urządzenia wytwarzające niezwykle silne impulsy pola elektromagnetycznego. Działają podobnie jak kuchenki mikrofalowe, tylko zamiast skupiać mikrofale wewnątrz nieprzenikalnej obudowy wysyłają skoncentrowaną wiązkę w wybraną stronę niszcząc półprzewodnikowe komórki pamięci komputera. Podobno koszt takich urządzeń, znanych też pod akronimami HERF (High Energy Radio Frequency) lub EMPT (Electromagnetic Puls Transmition) jest

całkiem niski. Niektóre obiekty wojskowe są zabezpieczone przed takim atakiem, ale banki, centra administracyjne czy lotniska nie mają żadnych zabezpieczeń. Nawet samochody zbytnio nafaszerowane elektroniką można łatwo uszkodzić przy pomocy bomby mikrofalowej, nie mówiąc już o samolotach. Atak terrorystyczny tego rodzaju jest więc rzeczą możliwą.