Andrzej Kmiecik

Postawy etyczne hakera i krakera

Ewolucja w naukach komputerowych tworzy nowe okoliczności i możliwości działania. To konstytuuje problem oceny etycznej działań związanych z użyciem komputera i korzystania z zasobów komputerowych. W związku z tym powstała etyka technologii informatycznej (Information technology ethics)[1] .

Ta ocena etyczna wygląda inaczej z punktu widzenia „podziemia komputerowego" (Computer Underground) a inaczej z punktu widzenia instytucji zajmujących się kwestiami bezpieczeństwa komputerowego.

Na „podziemie komputerowe" składa się szereg różnych subkultur określanych takimi mianami jak: hakerzy, krakerzy, phreakers, newbies, warez d00dz, „dzieciaki-skrypciaki", samuraje, itd. Członkowie tych subkultur różnią się postawami etycznymi. Skoncentrujmy się głównie na postawach i poglądach etycznych krakerów (crackers) na tle postaw i poglądów etycznych hakerów (hackers), jako że hakerzy i krakerzy są we wzajemnej opozycji. Jako zasadę porządkującą analizy przyjęto wyznaczniki moralności czynu, mianowicie: intencja, treść przedmiotowa, okoliczności[2]. Badania oparto głównie na tekstach i e-zinach zamieszczonych na znanych witrynach hakerskich, takich jak: Antionline, Anticrack, NewOrder, ElfQrin, HakingPl i typowo krakerskich jak Fravia, +ORC, FFF, CrackingPl[3]. Wykorzystano również słownik „Jargon file", którego autorem jest TURBOWEST[4],

Potocznie terminy „haker" (hacker), „kraker" (cracker) wywołują nastrój tajemnicy. Są to również terminy wieloznaczne. Kim są zatem ludzie ukrywający się pod tymi określeniami? Mówiąc ogólnie, są to przede wszystkim osoby dobrze znające technikę komputerową, systemy operacyjne, języki programowania. Inaczej te dwa słowa rozumieją dziennikarze, a inaczej społeczności komputerowego podziemia w Ameryce i w Europie. Przede wszystkim to media ukształtowały obraz hakera jako cyber-złodzieja, terrorysty, jako najgorszego z ludzi[5]. Jednak na przełomie lat 70. i 80. słowo to miało znaczenie pozytywne, które później uległo zmianie na negatywne. Kim są więc hakerzy?

W USA do dzisiaj toczy się dyskusja dotycząca różnicy pomiędzy hakerem a krakerem. Na tym obszarze można przyjąć dwie następujące definicje: 1) haker jest to „osoba zafascynowana arkanami wiedzy o komputerach. Często jest programistą. Wie dużo o systemach operacyjnych i językach programowania. Znajduje luki w systemach i przyczyny ich powstawania. Nieustannie zdobywa nową wiedzę i dzieli się nią z innymi. Co istotne, nigdy nie niszczy celowo danych, 2) kraker (włamywacz) jest to osoba, która „włamuje się lub w inny sposób narusza bezpieczeństwo komputera zdalnego. Po uzyskaniu nieautoryzowanego dostępu niszczy kluczowe dane, zamyka dostęp prawowitym użytkownikom i ogólnie przyczynia się do powstawania problemów. Krakera jest łatwo poznać: kierują nim złe pobudki"[6].

Można przyjąć te dwie definicje, gdyż ich treść jest podsumowaniem rozważań nad istotą hakerstwa w wielu tekstach publikowanych na stronach internetowych. Trzeba jednak pamiętać, że krakerzy nie zgodziliby się na powyższą definicję krakera. A poza

tym istnieje wiele typów hakerstwa. Anonimowy autor tych definicji sam zauważa ich nieostrość. A z kolei „Jargon file" podaje 8 znaczeń słowa „hacker". Dokładnie omawia je w swoim dokumencie „Elf Qrin"[7].

Powyższa definicja hakera wyraża to, co sami hakerzy w USA mówią o sobie. Jest to społeczność ekspertów programowania przyznających się do wspólnej kultury, którzy tworzyli pierwszy współdzielony komputer, sieć ARPAnet. Na określenie samych siebie członkowie tej kultury utworzyli termin „haker". Hakerzy zbudowali Internet, stworzyli system operacyjny UNIX, uruchomili Usenet. W tym sensie hakerami są: Richard Stallman – założyciel Fundacji Darmowego Oprogramowania (Free Software Foundation) i twórca projektu GNU; Dennis Ritchie, Ken Thompson, Brian Kernighan – twórcy systemu UNIX i języka C; Linus Torvalds – twórca Linuxa, klonu UNIX-a; Bill Gates i Paul Allen – założyciele Microsoftu[8]. Dlatego nie powinno nas dziwić, gdy na stronie Borland Community znajdziemy „kącik hakera" (hacker corners)[9] lub gdy niektórzy członkowie Fundacji GNOME, pracujący nad środowiskiem graficznym dla Linuxa, określają siebie mianem „hackera"[10]. Ci właśnie „rzeczywiści" hakerzy nazywają włamywaczy do komputerów i sieci telefonicznych krakerami. Podstawowa różnica między hakerem a krakerem – wg hakerów – polega właśnie na tym, że haker buduje nowe rzeczy, a kraker – niszczy.

Odpowiedź na pytanie, kim jest haker, oparto głównie na dwóch artykułach:, jednego, którego autorem jest TURBOWEST', „How to be a hacker?"[11] oraz drugiego, który napisał Valerio „Elf Qrin" Capello, „Being a Hacker"[12]. Filozofią hakera jest filozofia Zen. Aby stać się hakerem, trzeba rozwijać niektóre z następujących postaw: 1) musisz czuć dreszczyk fascynacji z rozwiązania problemu, 2) musisz być przekonany, że trzeba dzielić się zdobytą informacją, 3) nie powinieneś się nudzić lub harować – automatyzuj pracę, 4) anty-autorytarność, 5) postawa nie zastąpi kompetencji. Haker nie powinien się nudzić, gdyż jest twórczy. Natomiast anty-autorytarność nie jest tym samym co walka z wszelkimi autorytetami. Tak jak dzieci muszą być prowadzone przez jakiś autorytet, tak też haker musi się zgodzić na przyjęcie pewnego rodzaju autorytetu, aby zyskać na czasie w realizacji celu. Ludzie autorytarni dobrze się czują w atmosferze cenzury i tajemnicy. Nie dowierzają woli kooperacji i współdzieleniu się informacją – lubią „kooperację", którą oni sami kontrolują. Tak więc, aby zachowywać się jak haker, trzeba rozwijać instynktowną wrogość do cenzorstwa, tajemniczości. Również samo kopiowanie postaw nie uczyni hakerem. Stanie się hakerem wymaga inteligencji, praktyki, poświęcenia i ciężkiej pracy.

Można tu zauważyć, że ten „dreszczyk fascynacji z rozwiązania problemu" ma wiele wspólnych cech z pojęciem uskrzydlenia zwiazanego z procesem uczenia się, o którym to pojęciu pisze Daniel Goleman w książce „Inteligencja emocjonalna"[13].

Hakerem jest się wtedy, gdy inni uznają cię za takiego. Aby więc być uznanym przez innych za hakera, trzeba czynić następujące rzeczy: 1) pisać oprogramowanie open-source, 2) pomagać w testowaniu i debugowaniu oprogramowania open-source (początkujący powinni wziąć udział w testowaniu rozwijających się projektów i modyfikować je), 3) publikować użyteczne informacje na stronach internetowych lub w formie dokumentów FAQ (Frequently Asked Questions), 4) pomagać w utrzymaniu pracującej infrastruktury. Kultura hakerska pracuje właśnie dzięki wolontariuszom. Są to ludzie, którzy administrują listami mailingowymi, są moderatorami newsgroup (grup dyskusyjnych), archiwizują strony, rozwijają RFC i inne techniczne standardy. Tacy ludzie uzyskują szybko wielki szacunek. Każdy wie, że to pochłania mnóstwo czasu i że nie jest to „zabawa" jak z pisaniem programów. Wykonując ją, pokazuje się poświęcenie; 5) służba samej kulturze hakerskiej, na przykład przez pisanie wprowadzeń, jak się stać hakerem. Kultura hakerska nie ma liderów, lecz ma swoich kulturowych herosów, plemienną star-

szyznę, historyków i opowiadaczy. Ale trzeba sobie uświadomić, że hakerzy nie ufają krzykliwemu ego swojej plemiennej starszyzny. Raczej trzeba przyjąć postawę skromności co do swojego statusu.

To, kim ma być haker dobrze, oddaje manifest hakera znany pod dwiema nazwami: „The Hacker's Manifesto" lub „Conscience of Hacker", napisany 8 stycznia 1986 roku, którego autorem jest „Mentor LOD/LOH" Loyd Blankeship. Jest on dostępny w wersji angielskiej na stronie „Elf Qrina". Polskie, wierszowane tłumaczenie jest z 1999 roku, a tłumaczem jest Tomasz 'tsca' Sienicki[14].

Jakie umiejętności są wymagane, aby stać się hakerem? Postawa hakera jest istotna, ale umiejętności są tu jednak ważniejsze, trzeba je bowiem posiadać wpierw, zanim zacznie się marzyć o hakerstwie. Po pierwsze, trzeba znać kilka języków programowania. Aktualnie powinno się znać następujące języki: Python, Java, C/C++, Perl, LISP. Python jest mocnym językiem łatwym do nauczenia się, Java jest natomiast drugim językiem programowania po Pythonie, C/C++ jest potrzebny ze względu na systemy UNIX-owe i oprogramowanie open-source, Perl i Lisp są potrzebne ze względu na tworzenie aktywnych stron internetowych. Po drugie, należy zdobyć i nauczyć się używania jednego z klonów UNIX-a typu open-source. Kultura hakerska jest bowiem skoncentrowana na systemach Unix-owych, gdyż jest to system operacyjny Internetu i do nich jest dostępny kod źródłowy. Po trzecie, trzeba nauczyć się używać Internetu i programowania w HTML-u. Po czwarte, ważna jest znajomość języka angielskiego, gdyż jest to język kultury hakerskiej i Internetu. Np. Linus Torvalds jest Finem, ale swój kod źródłowy Linuxa komentował w języku angielskim, przez co ten system operacyjny stał się dostępny dla wszystkich.

Wiedząc teraz, kim są hakerzy, jakie są wymagania co do ich postaw i umiejętności, można zapytać się o zasady etyki hakerskiej. „Jargon file" zawierający hasło „hacker ethic"[15] podaje dwie następujące zasady:

1. „Przekonanie, że dzielenie się informacją jest dobrem i dlatego właśnie jest etycznym obowiązkiem hakerów dzielić się swoją wiedzą przez pisanie programów open-source oraz ułatwianie dostępu do informacji i zasobów obliczeniowych gdziekolwiek to jest możliwe";
2. „Przekonanie, że łamanie systemów dla zabawy i eksploracji jest etycznie OK tak długo, jak długo kraker zobowiązuje się nie kraść, nie niszczyć lub naruszać zaufanie".

Wg autora dokumentu obie powyższe „zasady etyki normatywnej" są uznawane przez hakerów. Jednak większość hakerów podpisuje się pod etyką w sensie (1) i wielu z nich decyduje się na tworzenie oprogramowania typu open-source (tzn. otwartych źródeł). Niektórzy idą dalej i twierdzą, że wszelka informacja powinna być wolna a jakakolwiek kontrola własności jest czymś złym. Taka jest filozofia leżąca u podstaw projektu GNU[16], utworzonego przez wymienionego wyżej Richarda Stallmana.

Z kolei etyka w sensie (2) jest bardziej kontrowersyjna. Uważa się bowiem, że sam akt krakowania (włamania) jest nieetyczny. Lecz przekonanie, że „etyczne" krakowanie wyklucza niszczenie, co najmniej reguluje zachowanie ludzi, którzy siebie określają jako „[wielce] łaskawy" kraker. W tej wizji może być jedną z najwyższych form hakerskiej grzeczności: a) złamać zabezpieczenia systemu i następnie b) wyjaśnić operatorowi systemu operacyjnego, jak to było zrobione i jak tę „dziurę" w systemie można by „zatkać.

Autor „Jargon file" dodaje, że największą manifestacją tej etyki hakera jest to, że prawie wszyscy hakerzy są aktywnie skłonni dzielić się swoimi technicznymi trikami, oprogramowaniem, zasobami obliczeniowymi z innymi hakerami. Olbrzymie takie współpracujące sieci jak Usenet, FidoNet, Internet mogą funkcjonować bez centralnej kontroli z powodu właśnie tej cechy. Zarazem polegają oni na wzmocnionym poczuciu wspólnotowości, która może być nieuchwytną największą wartością hakerstwa.

„Elf Qrin" zauważa, że haker opierający się na zasadzie etycznej (2) nie uważa włamania się do systemu komputerowego za akt przestępczy. Nie kieruje nim bowiem idea: zniszczyć „pokonanego", ale ciekawość, chęć eksperymentowania. Bo właśnie wola badania jest siłą napędową hakera.

Ile trzeba mieć lat, aby zacząć się uczyć hakerstwa? Ponieważ hakerstwo jest sprawnością, której można się nauczyć, nie ma więc ograniczeń wiekowych. Wydaje się, że większość ludzi, która jest tym zainteresowana, jest w wieku 15 - 20 lat. Ale są wyjątki w obu kierunkach[17]. Wg „Elf Qrina" proces uczenia się hakerstwa zajmuje około dwóch lat. Inny haker „Creeping Death"[18] przyznaje, że przez 3 lata zapoznawał się z Internetem i pracą sieci, a przez 10 lat programował.

Wskazuje się na kilka typów hakerów. Rozróżnia się dobrych hakerów (good hacker), czyli „hakerów w białych kapeluszach" (white-hat-hacker), oraz złych hakerów (bad hacker), czyli „hakerów w czarnych kapeluszach" (black-hat-hacker). Dobry haker to haker, który wykorzystuje swoje umiejętności do dobrych celów, na przykład do „polowania"[19] na pedofilów, do ochrony przed złymi hakerami. Zły haker wykorzystuje swoje umiejętności do złych celów, na przykład do kasowania plików, „zawieszania" pracy komputera, formatowania twardego dysku[20]. Na oznaczenie złego hakera używa się również określenia „haker ciemnej mocy" (dark-side hacker). Pierwowzorem tego określenia jest postać Dartha Vaadera z filmu George'a Lucasa „Gwiezdne wojny", który jest po „ciemnej stronie Mocy". Wyrażenie to ma pokazać, że są również hakerzy tworzący pewien rodzaj elity technologicznej – Rycerzy Jedi[21]. Prócz tego istnieją „Script Kiddies", czyli „dzieciaki skrypciaki" – osoby, które włamują się do sieci za pomocą programów skonstruowanych przez innych, nie rozumiejąc zasady działania tychże programów. Są również „samuraje" – „włamywacze" do wynajęcia, wiernie służący wynajmującemu ich.

Podsumowując można stwierdzić, że hakerstwo jest postawą i sprawnością, której trzeba się samemu nauczyć. Nie można nauczyć się hakerstwa od kogoś. O statusie w społeczności hakerów decyduje opinia innych, a nie pieniądze. Można też wyciągnąć wniosek, że o tym, czy haker jest dobry, czy zły, decyduje jego intencja.

Nie wiadomo, kiedy dokładnie nastąpiło pierwsze włamanie do systemu komputerowego. Najpierw zaczęło się od włamań do sieci telefonicznych. Tę grupę ludzi nazywa się phreakerami (czytaj: friiker), czyli „włamywaczami telefonicznymi". Phreakerzy prawdopodobnie przez przypadek włamali się do sieci komputerowej robiąc nasłuch połączeń telefonicznych. W latach 80. włamywaczami zostawali często utalentowani programiści. Wtedy pojawiły się trudności związane z odróżnieniem hakera od włamywacza (krakera), które trwają do dzisiaj[22]. Na różnych listach dyskusyjnych toczą się dyskusje związane z tym, kim jest haker i kim jest kraker[23].

Wg „Jargon file" kraker (cracker) to ktoś, kto łamie zabezpieczenia systemu. Termin ten został „ukuty" ok. 1985 roku przez hakerów z powodu nieporozumień dziennikarskich dotyczących pojęcia „hacker" . Dalej jest wzmianka, że krakerzy mają tendencję do zbierania się w małe, sekretne grupy. Prawdziwi hakerzy uważają ich za „oddzielną i niższą formę życia".

Powyższa definicja krakera (jak i hakera) odstaje mocno od rozumienia tego słowa na terenie Europy. Przez hakerów rozumie się tu włamywaczy do sieci komputerowych, a przez krakerów tych, co łamią różne zabezpieczenia programów komputerowych. Można to zauważyć, czytając tutory i e-ziny grup krakerskich w Europie.

Podstawowa różnica między krakerami a hakerami tkwi w tym, że kraker nie interesuje się zagadnieniami sieciowymi ani się na nich nie zna i nie jest to mu potrzebne. Krakerzy uważają, że hakerzy nie wiedzą, kim jest kraker. Kraker jest to osoba usuwająca zabezpieczenia programów, a nie – jak się sądzi – niszcząca serwery. Różnica między

hakerami a krakerami tkwi również w innych umiejętnościach. Hakerzy nie znają asemblera, który jest podstawowym językiem dla krakera. Kraker analizuje zdeasemblowany kod programu w celu znalezienia numeru seryjnego lub okna żądającego rejestracji programu[24]. Niektórzy krakerzy uważają nawet, że znajomość języków wyższego poziomu jak C/C++, Delphi jest pomocna przy usuwaniu zabezpieczeń, ale nie jest konieczna[25]. Z tym ostatnim zdaniem nie można się jednak zgodzić, gdyż współcześnie pisane programy korzystają z funkcji API Windows. Nieznajomość tych funkcji wręcz uniemożliwi analizę zdeasemblowanego kodu. Dlatego właśnie ważna jest znajomość systemu operacyjnego, dla którego pisany jest dany program. Ta znajomość systemu operacyjnego jest wspólną cechą hakerów i krakerów, jeśli chodzi o umiejętności.

Kraker ma do czynienia z następującymi zabezpieczeniami programów: a) standardowe jak nag-screen (okienko przypominające, że nie uiszczono opłaty rejestracyjnej), trial (ograniczenie czasowe), demo (wyłączone niektóre funkcje), rejestracja poprzez podanie numeru seryjnego, b) zabezpieczenia wzmocnione, takie jak sprawdzanie sumy kontrolnej, stosowanie procedur antydebugingowych, kompresja i szyfrowanie pliku wykonywalnego, zabezpieczenia przed kopiowaniem, klucze sprzętowe (tzw. dongle)[26].

Jakie są podstawowe narzędzia pracy krakera? Podstawowym narzędziem jest debugger SoftIce. Pozwala on śledzić wykonywanie się programu instrukcja po instrukcji w asemblerze, bez względu na język użyty w danym programie. Drugim narzędziem jest disasembler. Najbardziej popularny jest W32DASM, Sourcer. Do kompilacji zdeasemblowanego kodu używa się asemblerowego kompilatora TASM lub MASM. Trzecim potrzebnym narzędziem jest HEX-edytor. Dzięki niemu można wprowadzać na stałe zmiany do programu bez potrzeby jego ponownej kompilacji. Najbardziej popularne są tu HEX Workshop i Hacker's view. Są to narzędzia podstawowe. Pozostałe narzędzia służą do deszyfracji plików wykonywalnych, „zrzutu" programu z pamięci operacyjnej na dysk (tzw. dumpery) itp.[27]

Natomiast hakerzy w sensie włamywaczy zwykle używają różnych skanerów nasłuchujących połączeń modemowych, sniferów śledzących przepływ danych na serwerze i w ten sposób próbujących uzyskać np. hasła, „łamaczy" haseł, „koni trojańskich".

Jakie są natomiast wymagane podstawowe umiejętności? Wymagana jest znajomość asemblera, języka angielskiego oraz potrzebna jest intuicja[28]. Prócz tego trzeba posiadać umysłowość nie ukierunkowaną na zysk[29]. Język angielski jest potrzebny ze względu na FAQ-i (Frequently Asked Question) i tutory dotyczące usuwania zabezpieczeń programów[30]. Są to źródła pomocne w uczeniu się „krakowania" programów. Można znać różne schematy zabezpieczeń i wiedzieć, jak je „łamać", ale to nie czyni jeszcze krakerem. Potrzebna jest tu intuicja, „czucie kodu". Jeden z nieznanych autorów tutora krakowania, należący do znanej fińskiej grupy krakerskiej +ORC, mówi tu o czymś takim jak „zen-cracking". Wg niego kraking nie dotyczy programów komputerowych, ale informacji w nich zawartych. Krakowanie oznacza tu odrzucenie kontroli innych, pozwala czuć, że jest się wolnym. Kraker musi być zawsze zdolny wyjść poza to, co jest oczywiste, musi poszukiwać wiedzy[31].

Takie „czucie kodu" wytwarza się w wyniku długiej praktyki programistycznej i łamania zabezpieczeń. To właśnie „czucie kodu" i poszukiwanie wiedzy jest czymś wspólnym, jeśli chodzi o umiejętności, dla krakerów, „złych hakerów" i „dobrych hakerów". Powyższe wyznanie jednego z członków grupy +ORC wskazuje, że u podstaw ich działania leży ta sama zasada etyczna, do której odwołują się „dobrzy hakerzy" – że informacja jest wspólnym dobrem i trzeba się z nią dzielić.

Fakt, iż krakerzy uważają, że kraking nie dotyczy programów komputerowych, ale informacji w nich zawartych, wskazuje na ścisłe powiązanie krakingu z zagadnieniem reversingu (reverse engineering), tzn. odkrywania idei leżących u podstaw działania ja-

kiegoś programu komputerowego. Reversing jest przedmiotem sporów prawnych. Wydaje się, że przekonanie, iż informacja to dobro wspóle jest podstawą rozstrzygnięć sądowych na korzyść reversingu.

Kim są krakerzy ? Dlaczego niektóre osoby zajmują się łamaniem zabezpieczeń programów? Na to pytanie jest trudniej odpowiedzieć niż w przypadku hakerów. Krakerzy tworzą bowiem „narodowe sceny", tzw. „cracksceny". W Europie istnieje „crackscena" fińska (+ORC – Old Red Crackers), francuska (FFF), niemiecka (Y0da), hiszpańska (Whisky Kon Tekila – WKT), polska, rosyjska itd. „Sceny narodowe" specjalizują się w łamaniu zabezpieczeń danego typu. „Sceny" te są w różnym stopniu zjednoczone i różnią się spojrzeniem na aspekt etyczny swojej krakerskiej działalności. Można jednak stwierdzić, że łączy je wspólne przekonanie, iż dostęp do informacji powinien być wolny.

Na fińskiej „crackscenie" działa grupa +ORC. Teksty opublikowane przez tę grupę wskazują na motywy, które można określić jako anarchistyczne. Jest to wyraz sprzeciwu wobec społeczeństwa konsumpcji, wobec prawa i konwencji. Krakerzy nie łamią zabezpieczeń dla pieniędzy. Przedstawiciele tej grupy uważają, że programy powinny być „wolne" (free), dostępne dla każdego. Nie zgadzają się z tym, że można być programistą tylko po to, by „zagarniać" pieniądze. Prawdziwy kraker nie działa dla pieniędzy. Jest to postawa konieczna dla bycia krakerem. Jest to bunt wobec społeczności, w której żyją, bo życie w niej jest nacechowane egoizmem, jest to bunt wobec materialnych wartości. Tylko postawa nieuwikłania w wartości materialne doprowadzi do wiedzy „oświecenia" (satori) i pozwoli łamać zabezpieczenia w „prawy" sposób[32] . Postawa buntu doprowadziła do powstania przy tej grupie Uniwersytetu Krakowania, w skrócie +HCU (Higher Cracking University), założonego w kwietniu 1996. Jego twórcy noszą pseudonimy: NaTzGUL, Quine, Jack of Shadows. Ci, którzy spełnią wymagane warunki w czasie egzaminu, stają się członkami grupy +HCU. Prace tego „uniwersytetu" są dostępne na mirrorach „Fravii" rozmieszczonych w kilkunastu krajach świata[33].

Krakerzy odżegnują się od piractwa. Przykładem tego jest grupa AAOCG (Advanced Art Of Cracking Group), powstała kilka lat temu w Holandii. Istniała trzy dni. W jej skład wchodziły nie znane już dzisiaj trzy osoby. Ponowna reaktywacja grupy nastąpiła w lipcu 1999 roku. Jest to grupa osób, które mówią o sobie, że interesują się analizowaniem zabezpieczeń oraz ich łamaniem. Członkowie grupy podkreślają, że nie mają zamiaru pomagać w piractwie komputerowym a wszelkie materiały zawarte na tej stronie mają służyć wyłącznie celom edukacyjnym. Cracking jest traktowany przez nich jako sztuka. Analizowanie kodu programu jest rzeczą trudną, natomiast posiadanie tej umiejętności daje możliwości dokonywania licznych zmian w oprogramowaniu, często wbrew intencjom ich twórców. Członkowie grupy jednak zwracają uwagę na często pojawiające się wątpliwości natury etycznej: czy należy publikować gotowe cracki na stronach WWW? Jest to trudne pytanie dla nich, gdyż z jednej strony chcą zaprezentować własne prace innym, a z drugiej strony pamiętają o twórcach programów, ich ciężkiej pracy. Dlatego grupa zamieszcza cracki, mając nadzieję, że będą wykorzystane jedynie dla celów edukacyjnych. Dlatego pojawia się imperatyw hipotetyczny: „Jeżeli podoba Ci się program - KUP GO!!!"[34]. Ten imperatyw można bardzo często spotkać w plikach informacyjnych dołączonych do cracków tworzonych przez różne grup. Niektóre grupy nawet nie rozpowszechniają seriali, jeśli jakiś twórca programu poprosi o to[35]. Zwracam tu uwagę na to, że piractwem komputerowym zajmują się grupy typu warez d00dz. Rozprowadzają one pirackie oprogramowanie za niewielką cenę; charakteryzują się tym, że łamią zabezpieczenia komercyjnych programów w tym samym dniu, w którym ukazuje się wersja handlowa.

Jeśli chodzi o polską „crackscenę" to najczęściej wymienia się jako główną grupę CrackingPL[36].

Krakerzy – inaczej niż hakerzy – nie dzielą się na dobrych i złych. Często między krakerami występuje rywalizacja, jak w sporcie. Żaden kraker nie łamie zabezpieczeń dla sławy. Robi to dla osobistej satysfakcji, dla poszerzenia swojej wiedzy. Kraker jest skazany na życie w ukryciu. Dla niego kraking polega na mozolnym ślęczeniu nad kodem programu[37]. Lise Grim z francuskiej grupy FFF (Fighting For Fun) pisze, że krakerzy kierują się zasadą „wiedza to potęgi klucz". Pisze, że filozofia crackingu oparta jest na idei wolnej wymiany informacji i bezpłatności produktów. Dlatego krakerzy są bardzo odlegli od miejsc typu Warez, gdzie za niską cenę proponuje się komercyjne oprogramowanie, lub od Kaaza czy innych miejsc typu peer-to-peer[38].

Można zauważyć, że tak rozumiane krakerstwo ma wspólne idee z hakerstwem (dobrym). Chodzi tu szczególnie o wolność informacji i dzielenie się wiedzą. Za wspólną zasadę etyczną można uznać wymienioną wyżej zasadę (1). Różnica tkwi w treści przedmiotowej hakerstwa i krakerstwa. Nie można również powiedzieć, że wszystkie społeczności podziemia komputerowego są pozbawione zasad etycznych, że jest tu degeneracja etyki osobistej.

Kraking podlega ewolucji. Obecnie przechodzi się od łamania zabezpieczeń programów komercyjnych do badania „crackme". Są to programy mające różne zabezpieczenia, pisane przez jednych krakerów dla drugich[39]. Na wielu stronach nie umieszcza się już gotowych cracków, ale podaje się sposób złamania zabezpieczeń. W takim przypadku zainteresowana osoba musi posiadać odpowiedni zestaw narzędzi i wiedzę umożliwiającą samodzielne złamanie zabezpieczeń danego programu[40].

Dla celów wychowawczych ważne jest ustalenie wieku osób należących do podziemia komputerowego. Jeśli chodzi o włamania do sieci komputerowych, to ustalono, że typowy amerykański, „systemowy hacker" jest płci męskiej i jest w wieku 16 - 25 lat[41]. Z kolei w Polsce nie są to na pewno uczniowie szkół zawodowych. Są to uczniowie, którzy są znudzeni szkolnymi lekcjami informatyki[42]. Wspomniany wyżej Lise Grim pisze, że średnia wieku krakera to 25 - 26 lat i że jest osobą po studiach wyższych.

Na zakończenie zdanie anonimowego autora książki „Internet. Agresja i ochrona". Stwierdza on, że problem hakerów i krakerów jest dużo bardziej złożony, niż wskazują na to oskarżenia prokuratorskie. Uważa, że należy lepiej zrozumieć motywację tych jednostek, ich sposób życia[43]. Dlatego właśnie w ocenie etycznej krakingu trzeba też zwrócić uwagę na okoliczności, mianowicie na biedę panującą w wielu krajach, która zmusza do korzystania z pirackich programów komputerowych, gdyż cena wersji oryginalnych nie jest dostosowana do średnich zarobków w danym kraju. Istnieje również niebezpieczeństwo, że „etyka informatyczna" będzie skłaniała się ku etyce konsekwencjonalistycznej, tzn. osądzania czynów w terminach ich skutków lub w oparciu o aktualne krzywdy[44]. Szczególnie wtedy, gdy jako zasadę etyczną przyjmie się zasadę (2).

Przypisy

1. H. Nissenbaum, *Information technology and ethics*, in: E. Craig (gen. ed.) *Routledge Encyclopedia of Philosophy*, Routledge, London, New York 1998, vol. 4, s. 778 - 782.
2. T. Styczeń, J. Merecki, *ABC etyki,* Lublin 1996.
3. http://www.antionline.com – grupa ta dostarcza tutory, kody źródłowe wirusów i koni trojańskich; http://neworder.box.sk – dostarcza tysiące linków do innych stron hakerskich i krakerskich, zawiera magazyny hakerskie i krakerskie (tzw. e-ziny); http://www.elfqrin.com/.
4. http://www.tuxedo.org/~esr/faqs/hacker- howto.html; „Jargon file" jest też dostępny na stronie Elf Qrin'a.
5. P. Abrantez (Ghost_Rider), ezine, na stronie http://www.elfqrin.com/; hacker, znaczenie 8, w: Jargon file.
6. Autor anonimowy, *Internet. Agresja i ochrona*, tł. z ang. zbiorowe, Wrocław 1998, s. 63. W przedmowie autor przedstawia się jako Ben Elgin.
7. Being a Hacker, http://www.elfqrin.com/docs/BeingHacker.html.

8. Autor anonimowy, Internet. *Agresja i ochrona,* s. 71 - 72.
9. http://community.borland.com/.
10. Z. Chyła, *W pracowni GNOMA,* Linux+ 12/2002, s. 20.
11. TURBOWEST, how to be a hacker, http://www.antionline.com/showthread.php?s=&action==showpost&postid=570621. Jest to bardzo ważny dokument dostępny w kilkunastu językach: bułgarskim, katalońskim, chińskim (uproszczonym), chińskim (tradycyjnym), duńskim, francuskim, niemieckim, hebrajskim, węgierskim, indonezyjskim, włoskim, japońskim, koreańskim, portugalskim (Brazylia), portugalskim (Europa), rosyjskim, szwedzkim. O ile mi wiadomo, nie jest dostępny w języku polskim.
12. Valerio „Elf Qrin" Capello, Being a Hacker http://www.elfqrin.com/docs/BeingHacker.html;
13. D. Goleman, *Inteligencja emocjonalna*, Poznań 1997.
14. http://www.under.websex.pl/hack.html.
15. http://www.antionline.com/jargon/hackerethick.php.
16. http://www.gnu.org/. GNU znaczy "not Unix".
17. TURBOWEST, how to be a hacker.
18. Creeping Death, A Guide To Hacking and Its Culture, http://www.elfqrin.com/
19. Zob. historia Genocide'a, [w:] D. Verton, *Pamiętniki hakerów*, Warszawa 2002, s. 19 - 41.
20. W. Wang, *Internet, hakerzy, wirusy*, Warszawa 2001, s. 43, 314, 323. W tłumaczeniu polskim powyższe określenia wyraża się następująco: hakerzy w białych kapeluszach i odpowiednio – hakerzy w czarnych kapeluszach.
21. dark-side hacker, w: Jargon file.
22. Autor anonimowy, *Internet. Agresja i ochrona*, s. 69.
23. „Ennis", The Ultimate Newbie FAQ, http://www.antionline.com/showthread.php?s=&threadid=218093 What is a hacker....? http://www.antionline.com/showthread.php?s=1cb780530043722 25e55382a76945e7e&threadid=234264
24. „mNICH", Cracking-Reverse engineering, w: crack 5, http://www.underground.org.pl; "Ma-rYu-sH/CHInc", Kim naprawde jesteśmy - Crackerzy, www.cracking.pl.
25. http://onlinesecurity.virtualave.net/hacking/cracking.htm
26. P. Eerveò, *Cracking. Jak się przed nim bronić,* Warszawa 2001.
27. Cracking Tutorail, http://packetstormsecurity.org/. Narzędzia te są dostępne np. na stronie http://www.underground.org.pl/crack.html. B. Wójcik, *Jak utrudnić życie krakerowi?*, Software 2.0 9(93) 2002, s. 44-47.
28. „mNICH", crack 1, http://www.underground.org.pl.
29. How to crack - tutorial by +ORC - Lesson 1: an approach, http://neworder.box.sk/codebox.links.php?&key=orccracktu
30. http://cracking.home.ml.org/, http://neworder.box.sk/ – strony ta zawierają wiele aktualnych FAQ-ów i tutorów w języku angielskim.
31. How to crack - tutorial by +ORC - Lesson 2: tools and tricks of the trade, http://neworder.box.sk/codebox.links.php? &key=orccracktu
32. How to crack - tutorial by +ORC - Lesson 2: tools and tricks of the trade, http: //neworder.box.sk/codebox.links.php? &key=orccracktu
33. Np. http://fravia.anticrack.de/io13.htm. Polski mirror "Fravii" jest niedostępny. Prawdopodobnie został zdjęty z serwera. Link fravia.kilrathi.pl jest bowiem nieaktywny.
34. http://www.aaocg.prv.pl/.
35. Crackmag "BadIdea", www.badidea.prv.pl.
36. http://www.cracking.pl/.
37. „Ma-rYu-sH/CHInc", Kim jest kraker ?, www.cracking.pl
38. http://www.fighting-for-fun.fr.st/.
39. http://www.smola.prv.pl/.
40. Zob. np. www.anticrack.de, stronę fravii.
41. cracker.txt, http://www.antionline.com/index.php.
42. „AnGeL", Etyka Hackera, http://www.qdnet.pl/~angel/.
43. s. 64.
44. P.A.Taylor, them_and_us.txt, rozdział 6.3, http://www.elfqrin.com. Jest to część książki: Hackers: *A Study of A Technoculture,* Routledge and Kegan Paul 1998.