A N N A L E S
UNIVERSITATIS MARIAE CURIE-SKŁODOWSKA
LUBLIN - POLONIA
VOL. XVIII SECTIO J 2005

Wydział Pedagogiki i Psychologii
Zakład Psychologii Ogólnej

JAKUB LICKIEWICZ

Obraz hakera w oczach uczniów szkół średnich

The image of a hacker in the opinion of secondary school students

Idea urządzenia umożliwiającego szybki i tani przekaz informacji fascynowała ludzkość od początków cywilizacji. Aby ją osiągnąć, próbowano stosować różne środki, jednak dopiero rozwój technologii informatycznych umożliwił spełnienie tego marzenia. Pomysł połączenia ze sobą komputerów w sieć powstał już w trakcie „zimnej wojny", gdy amerykańska armia prowadziła badania nad możliwością dowodzenia i łączności w przypadku wojny nuklearnej. Celem tych eksperymentów było stworzenie sieci teleinformatycznej, mogącej działać pomimo zniszczenia jej części, np. wskutek wybuchu bomby atomowej (Sienkiewicz 2000). Jednak dopiero stworzenie w 1969 roku przez amerykańską agencję ARPA sieci złożonej z czterech komputerów umożliwiło rozwój idei szybkiej komunikacji. W ciągu następnych pięciu lat ARPAnet łączył już 35 ośrodków akademickich, stając się tym samym podstawową platformą komunikacji między nimi (Anonymous 2000). Kolejne lata przyniosły odkrycia będące przełomem dla rozwoju internetu i sprawiły, że stał on się jednym z najpopularniejszych sposobów komunikacji na całym świecie. Dzięki sieci teleinformatycznej granice państw utraciły jakiekolwiek znaczenie, a Ziemia stała się „globalną wioską". Jednak pomimo wolności przepływu informacji, każdy użytkownik sieci, a w szczególności organizacje rządowe, korporacje oraz banki dążą do zachowania części posiadanych przez nich danych do wyłącznego użytku osób zaufanych. Niestety, ich próby zachowania polityki prywatności pozostają często w sprzeczności z celami niewielkiej grupy użytkowników sieci, zwanych popularnie hakerami.

NIEJASNOŚCI TERMINOLOGICZNE WOKÓŁ HAKERÓW

Słowo „haker" przeszło długą ewolucję, zanim nabrało obecnego, funkcjonującego w społeczeństwie, negatywnego znaczenia. Jego pierwsze użycie datuje się na lata pięćdziesiąte XX wieku. Oznaczało wtedy osobę, którą cechowały szczególne zdolności w dziedzinie elektroniki. Dopiero później, wraz z rozwojem komputerów, studenci MIT (Massachusetts Institute of Technology - elitarna uczelnia techniczna) przejęli to słowo dla określenia wybitnych programistów. W latach siedemdziesiątych XX wieku mianem hakerów nazywano elitę, która nie tylko potrafiła pisać programy, ale czyniła to w sposób niemal idealny. W tym czasie określenie kogoś tym pojęciem było dowodem szacunku (Williams 1999). Do dziś wielu programistów uważa się za hakerów w tym właśnie rozumieniu tego słowa. Lata osiemdziesiąte ubiegłego wieku przyniosły stopniowe upowszechnienie komputerów, powstała wówczas nowa subkultura, rządząca się swoistą etyką i zasadami - sformułowano postulat wolności wszelkiej informacji oraz uwierzono w możliwość tworzenia sztuki i piękna przy pomocy komputera (Levy 1994). Jednak coraz powszechniejszy dostęp do sieci sprawił, że powstała pewna grupa jej użytkowników, którzy sprzeniewierzyli się tym zasadom i zaczęli wykorzystywać swoją wiedzę w celu włamywania się do systemów, wykradania danych lub ich niszczenia. Sami hakerzy określają ich mianem crakerów (Raymond 2001).

Hakerzy postrzegają siebie jako osoby, które bardzo dobrze opanowały języki oprogramowania, umieją łamać zabezpieczenia komputerów i robią to, ale wyłącznie w celach poznawczych, nigdy destrukcyjnych. Ich celem jest pogłębianie własnej wiedzy oraz chęć ulepszania zabezpieczeń komputerów. W tej specyficznej subkulturze nie ma znaczenia niszczenie, lecz wiedza, która daje szacunek i respekt wśród innych użytkowników sieci (Doroziński 2001). Himanen zauważa, że postępowanie hakerów zdominowane jest przez dążenie do wolności, radość z eksploracji oraz zapał do pracy, którą jest zgłębianie coraz to nowych systemów komputerowych (Himanen 2001). Z kolei Chandler (1996) wyróżnia etapy ewolucji pojęcia hakera w mediach, podając oryginalne, omówione już wcześniej, rozumienie tego słowa jako „komputerowego czarodzieja". Z czasem - jak wspomniałem - pojęcie to ewoluowało, głównie za sprawą zasad, które wymienia Levy, w swoistego anarchistę i elektronicznego renegata, sprzeciwiającego się zasadom komercji rządzącym w sieci. Następnie wraz z upowszechnianiem sieci pojawili się zapaleńcy czerpiący radość z krążenia po sieci, ich celem było jedynie dotarcie do jak największej liczby miejsc. Dopiero później pojawił się obraz hakera jako mordercy i przestępcy, posiadającego dość umiejętności i odwagi, by dzięki komputerowi okraść bank, a nawet wywołać wojnę nuklearną. Niejako w konsekwencji zaczęto traktować hakerów jako osoby uzależnione od komputera, które należałoby z tego nałogu leczyć. Ostatnio pojawiło się rozumienie hakera jako szpiega, osoby, która jest w stanie przeszukiwać zastrzeżone bazy danych, wykradać informacje, a następnie

sprzedawać je tym, którzy są w stanie za nie zapłacić. Chandler słusznie zauważa, że obecne rozumienie tego pojęcia ma wymiar głęboko negatywny. Hakerzy obwiniają za ten stan rzeczy crakerów, którzy mają być odpowiedzialni za wszelkie szkody, jakie ponoszą użytkownicy sieci - od tych korzystających z komputerów w domu, do właścicieli wielkich korporacji.

Tymczasem problem rozumienia samego pojęcia związany jest z faktem, iż różne środowiska odmiennie widzą działalność hakerów i jej skutki. Według organów ścigania i osób zajmujących się bezpieczeństwem sieci są to kryminaliści, których aktywność należy ograniczać. Obraz, kreowany przez media w filmach i książkach, jest dosyć niejednoznaczny, gdyż z jednej strony haker przedstawiany jest jako człowiek mogący uratować świat, a z drugiej -jako osoba dążąca do jego zniszczenia. A zatem obraz hakera w społeczeństwie jest uzależniony głównie od faktów przedstawianych przez media, które najczęściej prezentują negatywny aspekt ich aktywności. Sami hakerzy uważają siebie najczęściej za miłośników komputerów i osoby doskonalące zabezpieczenia sieci (Lieberman 2003).

Hakerzy wydają się subkulturą bardzo wewnętrznie zróżnicowaną, co sprawia, iż zaproponowano wiele różnych klasyfikacji (Sterling 1992, Denning 1990, Hafner i Markoff 1995). Szczególnie interesujące są rozważania Rodgersa, który wyróżnia siedem grup hakerów, w zależności od ich doświadczenia i obszaru zainteresowań. Początkujący określani są mianem dzieciaków (nazywani są też czasem *script kiddies),* korzystają wyłącznie z gotowego oprogramowania i instrukcji, które można znaleźć w sieci. Cyberpunki to osoby, które potrafią same napisać potrzebne im oprogramowanie, ale ich wiedza jest ograniczona - to właśnie oni biorą często udział w czynach przestępczych. Kolejną grupę stanowią byli pracownicy firm, którzy z zemsty atakują swoje miejsce zatrudnienia. Jeszcze inni to programiści, których umiejętności są tak duże, że mogą pisać programy wykorzystywane później przez innych hakerów w swojej działalności. Można również wyróżnić stosunkowo nieliczną grupę, która cały czas przestrzega ideologii początków tego ruchu, ceniąc sobie aspekt intelektualny i poznawczy hakowania. Ostatnie dwie grupy - powstałe stosunkowo niedawno - to profesjonalni kryminaliści i cyberterroryści.

HAKER W WYBRANYCH TEORIACH PSYCHOLOGICZNYCH

Problematyka związana ze zjawiskiem hakerstwa nie została do tej pory dokładnie zbadana przez psychologów. Pomimo licznych prób „profilowania" znanych hakerów przez autorów książek popularnonaukowych i biografistów (m.in. Bowcott, Hamilton 1993, Goodell 1996, Stoll 1998) dotychczasowy dorobek psychologii w tej materii jest niewielki. Większość doniesień z zakresu motywacji i osobowości hakerów opiera się na ankiecie przeprowadzonej przez nich samych w latach dziewięćdziesiątych XX wieku. Wzięło w niej udział około 100 osób ze Stanów Zjednoczonych. Według ankiety haker jest najczęściej

mężczyzną, interesuje się naukami ścisłymi, cechuje go inteligencja i doskonała pamięć oraz niechlujny charakter pisma. Preferują raczej wygodny ubiór, pracę w nocy i rzadko używają substancji psychoaktywnych (Russ 2002). Mimo iż ten profil jest często cytowany zarówno w prasie, jak i literaturze popularnonaukowej, nie został dotychczas dokładnie zweryfikowany empirycznie. Pewnym potwierdzeniem powyższych stwierdzeń jest praca Chantlera (1995), który po przebadaniu 23 hakerów sklasyfikował ich w trzy grupy: 1) inteligentnych, błyskotliwych i dobrze wykształconych, 2) błyskotliwych ze słabym wykształceniem oraz kontrowersyjnymi zasadami moralnymi i etycznymi, 3) młodych i niedoświadczonych. Chantler stwierdza, że hakerzy zaczynają swoją działalność około 15 roku życia. Lieberman (2003) potwierdza tę zależność, dodając, iż jego badani często mieli w swoich szkołach problemy wychowawcze związane z nieprzestrzeganiem zasad, które próbowano narzucać im w trakcie procesu edukacyjnego. Z kolei, jak wykazują badania Voiskounskego i Smyslovej (2003), w tej grupie można znaleźć najczęściej początkujących hakerów, których według klasyfikacji Rodgersa określa się mianem *script kiddies*.

PROBLEMATYKA BADAŃ WŁASNYCH

Celem podjętych przeze mnie badań było zbadanie obrazu hakera w oczach uczniów szkół średnich. Równocześnie, opierając się na wcześniej zaprezentowanych badaniach, przyjąłem założenie, iż wśród uczniów szkół średnich można znaleźć osoby, które stawiają pierwsze kroki jako hakerzy. Dlatego też zdecydowałem się na badania wśród młodzieży klas licealnych, przypuszczając, iż to właśnie ta grupa jest najbliżej idei „społeczeństwa informacyjnego".

W związku z powyższym przyjąłem następujące założenia:

1. Istnieje jasny obraz hakera wśród uczniów szkół średnich, który pozwoli na stworzenie jednoznacznej definicji tego zjawiska.
2. Uczniowie klas informatycznych bardziej pozytywnie oceniają hakerów niż ich rówieśnicy z innych profilów klas.
3. Wśród młodzieży szkół średnich o profilu informatycznym można znaleźć osoby, które zaczynają hakować.

METODY BADAWCZE

Aby sprawdzić prawdziwość tych założeń, w grupie kontrolnej zastosowano ankietę, w której osoby badane miały odpowiedzieć na pytanie „Kto to jest haker?". Grupie tej nie dano do wypełnienia testu wiedzy, kierując się założeniem, iż hakerzy to głównie osoby zainteresowane naukami ścisłymi i informatyką. Grupa badana otrzymała do wypełnienia test wiedzy o internecie, napisany przeze mnie na podstawie lektury specjalistycznych podręczników oraz magazynów dotyczących hakowania. Następnie pytania testu zostały skonsul-

towane i poprawione przez wieloletnich administratorów sieci komputerowych. Test wiedzy składał się z 10 pytań, wśród których kilka zawierało dwie możliwości odpowiedzi - w zależności od poziomu umiejętności badanego w sferze internetu. Poziom trudności testu ustalono na podstawie analizy podręczników do nauki informatyki w szkole średniej. Ostatnie pytanie było powtórzeniem pytania z grupy kontrolnej. Test oceniano na skali trzypunktowej, stawiając 0 punktów za brak odpowiedzi, 1 za odpowiedź na poziomie programu nauczania szkoły średniej oraz 2 za odpowiedź świadczącą o wyjątkowej wiedzy w zakresie informatyki. Wynikiem testu była suma punktów, zawierająca się w przedziale 0-20 punktów. Test wraz z wariantami odpowiedzi przedstawiono w tabeli 1.

Tab. 1. Test wiedzy o internecie wraz z wariantami odpowiedzi
Test of knowledge about the Internet and variants of responses

Nr	Pytanie	Odpowiedź
1.	Co było najpierw: IP chains czy IP tables?	IP chains (pytanie dotyczy historii rozwoju sieci) (2 pkt. za prawidłową odp.)
2.	Podaj typowy port usługi SMTP i SSH?	SMTP: 25 SSH: 22 (pytanie dotyczy połączeń pocztowych, często atakowanych przez hakerów – po jednym punkcie za prawidłową odp.)
3.	Zaznacz, co nie jest nazwą protokołu: TCP/IP, FTP, UPS, NFS, UTP	UPS, UTP (znajomość protokołów jest niezbędna do dokładnej eksploracji sieci – po jednym punkcie za prawidłową odp.)
4.	Czy skanowanie portów to to samo co skanowanie antywirusowe?	Nie (skanowanie portów informuje użytkownika o próbie włamania do jego komputera) (1 pkt za prawidłową odp., 2 – za wyjaśnienie)
5.	Na czym polega sniffing?	Technika hakerska, służąca do podsłuchiwania informacji przesyłanych siecią (2 pkt. za prawidłową odp.)
6.	Co to jest 2600?	Prędkość procesora w MHz (1 pkt) najpopularniejsze hakerskie czasopismo (2 pkt.)
7.	Jakiego rodzaju programem jest Prosiaczek?	Koń trojański (program służący do przejęcia kontroli nad komputerem ofiary, jego twórca pracował w Lublinie, 2 pkt. za odp.)
8.	Co to jest DoS i na czym polega?	DOS to tekstowy system operacyjny (1 pkt.) DoS to atak hakerski Denial of Service blokujący komputer (2 pkt.)
9.	Co to jest Deamon?	Deamon Tools – popularny program służący do tworzenia wirtualnych dysków (1 pkt.) Deamon – typ programu w systemie UNIX, działa samodzielnie bez nadzoru, wykonując pewne funkcje (2 pkt.)
10.	Kto to jest haker?	(2 pkt. za odp.)

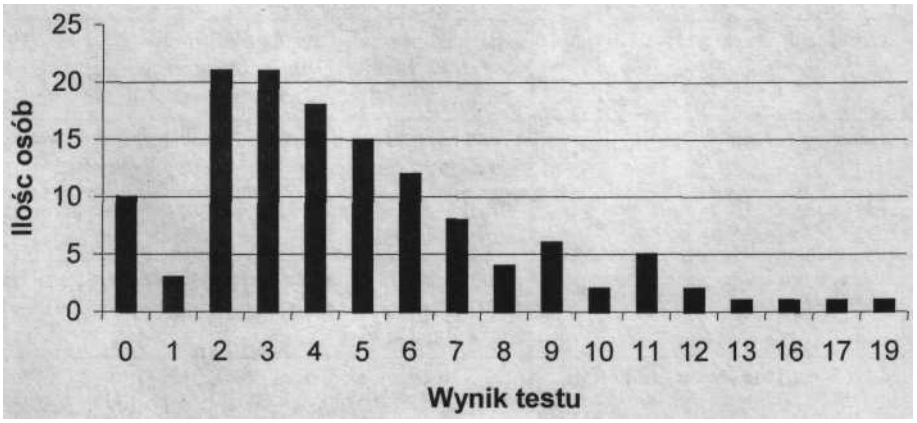
OSOBY BADANE. PROCEDURA BADAWCZA

Badaniami objęto 225 uczniów dwóch lubelskich liceów w wieku 15-19 lat. Grupę kontrolną składającą się z 94 osób (51 kobiet i 43 mężczyzn) stanowili uczniowie klas o zróżnicowanych profilach: europejskim, z międzynarodową maturą oraz menadżerskim. Grupą eksperymentalną było 131 osób (42 kobiety i 89 mężczyzn) z klas o profilu informatycznym.

Badania przeprowadzano w czasie trwania zajęć lekcyjnych, prosząc o pomoc w pisaniu pracy dotyczącej wiedzy na temat internetu. Uczniów zapewniono o anonimowości, prosząc o wpisanie w arkuszach wyłącznie informacji o płci, wieku oraz profilu klasy. Po wyjaśnieniu instrukcji badani przystępowali do rozwiązywania testu, co zajmowało im około 15 minut.

WYNIKI BADAŃ WŁASNYCH

Oceniając częstość występowania odpowiedzi w poszczególnych definicjach, pogrupowano je w kategorie dotyczące różnych cech, jakie - zdaniem badanych - prezentują hakerzy. W grupie badanej wyłączono 17 wyników ze względu na brak odpowiedzi na postawione pytanie. Wyniki obu grup przedstawiono w tabelach 2 i 3. Na wykresie 1 przedstawiono wyniki testu wiedzy o internecie grupy badanej.



Wykres 1. Wyniki testu wiedzy o internecie (n = 131)
Results of the test on the knowledge about the Internet

Tab. 2. Kategorie odpowiedzi na pytanie „Kto to jest haker?" (grupa kontrolna)
Categories of response to the question "Who is a hacker?" (control group)

Kategoria	Przykłady odpowiedzi (w nawiasie procent odpowiedzi)
Posiadane umiejętności	Dobrze zna komputer, ma często wybitne umiejętności komputerowe i informatyczne, tworzy programy, zna internet, informatyk z dużym doświadczeniem (38%)
Aspekt prawny	Wykorzystuje swoją wiedzę niezgodnie z prawem, kradnie dane, popełnia przestępstwa za pomocą sieci (34%)
Zakres działalności	Łamie hasła, kody, zabezpieczenia, strony internetowe, włamuje się na cudze komputery, wyszukuje luki w systemach (63%)
Motywacja (aspekt pozytywny)	Czerpie z tego przyjemność, robi to dla sportu, dla własnej satysfakcji, nie dla zarobku, to jego hobby, chce pokazać, co potrafi, sprawdza się, sam fakt łamania granic (11%)
Motywacja (aspekt negatywny)	Zaspokaja wybujałe *ego*, robi to z braku atrakcji w życiu realnym, wkracza w myśli i uczucia innych, robi to, bo na co dzień nie jest doceniany przez otoczenie (4%)
Aspekt materialny	Dokonuje przelewów pieniężnych na swoją korzyść, uzyskuje korzyści dla siebie, także materialne, okrada banki (8%)
Inne aspekty działalności	Wynajmowany do pracy, chroni innych przed utratą danych, pomaga je odzyskać, wynajmowany przez firmy (8%)
Haker a craker	Nie niszczy zasobów, niekoniecznie działa w celach przestępczych (14%)
Negatywne skutki działań	Szkodzi innym, narusza zasady, wywołuje zamieszanie i straty finansowe, zniszczenia wśród firm (15%)
Cechy psychiczne	Bardzo inteligentny, biegły w naukach ścisłych, pasjonat, kreatywny, twórczy (8%)
Synonimy	Przestępca komputerowy, włamywacz komputerowy, złoczyńca (4%)
Inne	Marnują czas, wyróżniają się ze społeczeństwa, nigdy nie ujawnia się przed innymi, chce omijać obowiązujące zasady (11%)

WNIOSKI

Jak wynika z uzyskanych informacji, pojęcie hakera nie jest zależne od profilu klasy. Wśród uczniów nie ma znaczących różnic w rozumieniu tego słowa. Tylko nieliczna grupa osób zauważa wieloznaczność pojęcia „haker", a także widzi różnice pomiędzy hakerem a crakerem. Natomiast większość badanych zauważa wyłącznie negatywne aspekty jego działalności, takie jak niszczenie danych, uszkadzanie komputerów i włamania do firm. Zaskakujące jest to, że definicje

Tab. 3. Kategorie odpowiedzi na pytanie "Kto to jest haker?" (grupa eksperymentalna)
Categories of response to the question "Who is a hacker?" (experimental group)

Kategoria	Przykłady odpowiedzi (w nawiasie procent odpowiedzi)
Posiadane umiejętności	Doskonale zna się na sprzęcie i systemach operacyjnych, potrafi wykorzystać możliwości komputera, mistrzowsko i bez ograniczeń porusza się po internecie (28%)
Aspekt prawny	Postępuje niezgodnie z etyką moralną, działa na granicy prawa (21%)
Zakres działalności	Blokuje konta, przejmuje władzę nad cudzym komputerem, pozyskuje informacje, kopiuje programy i gry komputerowe, włamuje się do firm (75%)
Motywacja (aspekt pozytywny)	Sprawdza własne umiejętności, chce pokazać, że zabezpieczenie jest skuteczne (6%)
Motywacja (aspekt negatywny)	Robi to ze zwykłej wredoty, dla własnych potrzeb oszukuje innych (1%)
Aspekt materialny	Robi to dla własnego wzbogacenia się finansowego (13%)
Inne aspekty działalności	Szuka błędów w oprogramowaniu, sprawdza bezpieczeństwo serwera, dąży do poprawy bezpieczeństwa w sieci (1%)
Haker a craker	Nie robi nic złego, wykorzystuje programy do nielegalnych (wg oficjalnego prawa) celów (7%)
Negatywne skutki działań	Narusza prywatność, niszczy dane, działa w złych celach i intencjach (12%)
Cechy psychiczne	Działa z rozmysłem (1%)
Synonimy	Złodziej, oszust internetowy (1%)
Inne	Komputer jest jego celem życia, potrafi na siebie zarobić nie wychodząc z domu, nie sposób ograniczyć jego działania, korzysta głównie z własnego oprogramowania (7%)

podawane przez badanych z obu grup niewiele się różnią. Wydawało się, iż uczniowie klas informatycznych, lepiej zaznajomieni z problematyką bezpieczeństwa sieci, powinni mieć bardziej pozytywny obraz hakera niż ich rówieśnicy z klas o innych profilach. Nieprawdziwość tego twierdzenia może być związana z faktem, iż niewielka liczba badanych miała dostateczną wiedzę, aby należeć do tej specyficznej subkultury, w której dąży się do coraz większego doskonalenia swoich umiejętności. Stąd mają oni obraz hakera, który pokrywa się z obrazem tworzonym przez media, a więc postrzegają go jako przestępcę komputerowego i włamywacza. Niewielka część osób zauważa jednak niejednoznaczność jego działalności, fakt częstej pracy nad poprawą bezpieczeństwa sieci czy też szukaniem luk w programach. Badani mają również podzielone zdanie na temat motywacji postępowania hakerów - część twierdzi, iż wynika

ona z niskiej samooceny, inni natomiast, iż jest sposobem sprawdzenia samego siebie i swoich umiejętności. Równocześnie, opisując cechy psychiczne hakera, badani potwierdzają pewne tezy wcześniej cytowanych badań, postrzegając hakerów jako osoby inteligentne i kreatywne, o dużych zainteresowaniach w kierunku nauk ścisłych, szczególnie matematyki. Niektórzy badani widzą w hakerach buntowników, inni osoby uzależnione od komputera i nieporadne w realnym życiu. W przedstawionych tu definicjach możemy zatem znaleźć wszystkie aspekty poruszane dotychczas w literaturze przedmiotu, co świadczy wbrew przyjętym początkowo założeniom o niejednoznaczności tego pojęcia.

Zebrany materiał pozwala na stworzenie definicji hakera, uznaną za jego obraz u większości uczniów liceów bez względu na profil. Według niej haker to osoba doskonale znająca się na komputerach, informatyce oraz internecie, postępująca niezgodnie z prawem, ponieważ łamie kody i zabezpieczenia, włamuje się do cudzych komputerów oraz niszczy lub kradnie dane zarówno firm, jak i osób prywatnych, często w celach majątkowych, a czasem dla zabawy.

Do interesujących wniosków prowadzi analiza testu wiedzy uczniów klas o profilu informatycznym. Wskazuje ona na niski poziom wiedzy z zakresu informatyki. Udało się jednak znaleźć trzech chłopców, którzy posiadali wystarczający zasób wiedzy, aby określić ich mianem początkujących hakerów. Osoby te wykazały się wiedzą wystarczającą do tego, aby dokonywać włamań do cudzych komputerów. Pozwala to na bardzo istotny wniosek, iż w każdej klasie o tym profilu można znaleźć przynajmniej jednego ucznia, który posiada takie szczególne - jak wskazują wyniki testu - zdolności. Potwierdza to wcześniej cytowane badania, które wskazywały na fakt, iż hakerzy zaczynają działać już w okresie szkoły średniej, a należy zakładać, że wraz z rozwojem technik informatycznych, ta średnia wieku będzie się stale obniżać. Według klasyfikacji Rodgersa są to zapewne dopiero *script kiddies,* ich działalność, jeśli nie zostanie prawidłowo pokierowana, może ewoluować w stronę działań niebezpiecznych dla innych użytkowników sieci. Ogromna odpowiedzialność spoczywa tu na nauczycielach, którzy powinni w ten sposób pokierować tymi młodymi ludźmi, aby zapobiec szkodliwym dla innych działaniom. Można to czynić poprzez zakładanie szkolnych klubów dla wybitnie uzdolnionych w tym kierunku uczniów lub też poprzez zajęcia z zakresu etyki sieciowej. Problem ten wydaje się szczególnie istotny w czasach rozwoju społeczeństwa informatycznego i z pewnością będzie narastał, jeśli odpowiednie kroki nie zostaną podjęte już teraz.

BIBLIOGRAFIA

Anonymous, *Historia internetu,* http://www.digitalaxt.pl stan na: 17.01.2005. Bowcott O., Hamilton S. (1993). *Hakerzy. Włamywacze i komputery.* Warszawa: Oficyna Wydawnicza Alma-Press. Chandler A. (1996). The changing definition and image of hackers in popular discourse. *International Journal of Sociology and Law,* 24, 229-254. Chantler N. (1995). *Risk: Profile of Computer Hacker.* Rozprawa Doktorska, Curtin University of technology, School of information systems.
Denning D. (1990). *Information Warfare and Security.* Boston: Addison-Wesley. Doroziński D. (2001). *Hakerzy. Technoanarchiści cyberprzestrzeni.* Gliwice: Helion. Goodel J. (1996). *Haker i samuraj.* Gdańsk: GWP. Hafner K., Markoff J. (1995). *Cyberpunk: outlaws and hackers on the computer frontier.* New York: Simon and Schuster.
Himanen P. (2001). *The Hacker Ethic and a Spirit of Information Age.* Random House.
Lieberman B. (2003). *Computer hackers. An Interactive Problem and what to do about it.* Research and Policy Memorandum, 301.1.
Levy S. (1994). *Hackers: Heroes of Computer Revolution.* London: Penguin Books. Raymond E. (2001). *The new hacker's dictionary,* http://home.nvg.org/~venaas/jargon/jargon_toc. html stan na: 09.07.2002. Rodgers M. (1999). *A new hackers taxonomy,* http://www.mts.net/~mkr/hacker.doc stan na: 17.01.2003. Russ W. (2002). *Change your personality,* http://www.secretguide.net/read/index.php stan na: 19.02.2003. Sienkiewicz S., *Historia internetu,* http://www.wodip.opole.pl/~ssienkiewicz/internet.html stan na: 15.01.2005. SterlingB. (1992). *The hacker crackdown: law and disorder on the electronic frontier.* London: Penguin Books.
Stool C. (1998). *Kukulcze jajo.* Poznań: Rebis.
Williams S., *W obronie wolności,* http://helion.pl/ksiazki/wobron.html stan na: 12.11.2004
Voiskounsky A. E., Smyslova O. V. (2003). Flow-based model of computer hackers motivation. *Cyberpsychology & Behavior,* 6, 171-180.

SUMMARY

The problem of computer hackers has not arisen enough interest of the psychologists so far. The article discusses the image of a hacker as perceived by investigators, society, media and hackers themselves. There have also been discussed stages of development of the very notion and has been presented the classification of the phenomenon. The outcome of the research dealing with the image of a hacker among students of secondary school with social and computer profile has been shown. No differences have been found between the above two groups with regard to the notion of a hacker, however, the data were sufficient enough to define the notion of a hacker. The article also discusses the results of the test on the knowledge of the Internet which aimed to indicate those with proper predisposal and knowledge in this respect. A group of boys presenting with such abilities has been selected. Finally, ways of preventing negative effects of this phenomenon have been suggested.