

АКТУАЛЬНЫЕ ПСИХОЛОГИЧЕСКИЕ ПРОБЛЕМЫ КИБЕР-ЭТИКИ

А.Е. Войскунский, А.И. Нафтульев

Статья посвящена обсуждению новейших тенденций в кибер-этике, её взаимосвязи с психологией и практикой образования. Ставится проблема обучения Интернет-пользователей новых поколений основам кибер-этики. Его главная задача состоит в том, чтобы адаптировать традиционную систему моральных суждений к условиям анонимного применения Интернета.

ACTUAL PSYHOLOGICAL PROBLEMS OF CYBER-ETHICS

A.E.Vojksunskij, A.I. Naftuljev

The article is devoted to discussion of the newest tendencies in cyber-ethics, its interrelations with psychology and practice of education. The problem of training of Internet - users of new generations to bases of cyber-ethics is put. Its main task will be to adapt traditional system of moral judgments for conditions of anonymous application of the Internet.

Кибер-этика: текущие исследования

Хотя этика является одной из древнейших сфер знания, прогресс современных технологий способствует появлению новых практических приложений, а именно так называемой кибер-этики. Под кибер-этикой, как правило, понимаются правила нравственного (т.е. правильного, честного, справедливого) поведения в среде Интернета. Она простирается далеко за пределы «сетевого этикета» – правил, выработанных в ранний период использования Интернета. В наши дни кибер-этика распространяется на коммуникативные (чаты, форумы, блоги и др.) и некоммуникативные сервисы, в т.ч. совместную работу, онлайн-игры, покупки или приобретение/продажу биржевых акций.

Особенности сегодняшней стадии развития кибер-этики до сих пор осознаны далеко не полностью. Большинство авторов отмечают про-

блемы, связанные с преступлениями, безопасностью и защищенностью; приватностью и личной свободой, порнографией, домогательствами и жульничеством, защитой детей от ущерба, наносимого Интернетом, хакерством, использованием чужих кредитных карт, пиратским использованием ПО, применением сети правыми и левыми экстремистами, шантажом и спамом, плагиатом, «фишингом», флеймом и т. д. [1–5]. Недавно появились и новые проблемы, связанные с этикой онлайн-исследований, в которых принимают участие люди [6–8].

Во многом сходные проблемы поднимаются и в сетевых ресурсах (cyberethics.cbi.msstate.edu/biblio/, www.cpsr.org/program/ethics/ и т.п.). В дополнение к универсальным нравственным принципам были разработаны и постоянно дополняются кодексы профессиональной этики. Стоит упомянуть кодексы профессионального поведения [9, 10], в частности, в сфере кибернетики и управления информационными системами [1, 11–13]. Кроме того, выработанный в АСМ (Association for Computing Machinery) Кодекс нравственного и профессионального поведения (<http://www.acm.org/constitution/code.html>) является полезным и широко обсуждаемым источником, равно как и кодекс Американской Психологической Ассоциации (APA), который в недавнее время подвергался пересмотру (<http://www.apa.org/ethics/>).

В силу своей значимости вопросы кибер-этики и профессиональные этические кодексы подробно обсуждались в профессиональных сообществах, проводились эмпирические исследования. Так, например, незаконные действия, связанные с использованием ПК (от незаконного копирования пиратского ПО до изменения/воровства данных с чужих ПК), широко распространены и часто осуществляются учениками средней школы: это наглядно показано в исследованиях, которые были проведены в калифорнийском городе Сан-Диего [14]. Руф и Томас [15] продемонстрировали, что студенты университетов с готовностью идут на ложь (незаконный доступ к электронным учебникам, скачивание и продажа музыкальных CD, копирование ПО), получая при этом весьма незначительную выгоду. Неудивительно, что имеется множество факторов, способных селективно воздействовать на подобное поведение. Аналогичное наблюдение сделано в работе [11]: на процесс нравственного выбора в ИТ-среде влияют различные комбинации юридических и профессиональных факторов или факторов, относящихся к сфере личных убеждений (религиозные, нравственные ценности, опыт) и социальному окружению.

Принято считать, что важным фактором также являются культурные особенности. Было показано, что частные религиозные представления (такие, как вера в череду перевоплощений, распространенная в Индии)

влияют на вероятность пиратства ПО и нарушения прав частной собственности в сфере ИТ [16]. Исследования, проведенные в Корее, показали значение пола, возраста и положения в социальной иерархии для морального выбора среди взрослых респондентов [17].

Отношение к нарушениям нравственности в сфере ПК/Интернета также может сильно варьироваться в зависимости от культуры [18]. Тем не менее исследования показали, что отношение к нарушению условий лицензии ПО, условий корпоративного пользования ПО, к распространению вирусов существенно различается у профессионалов, представляющих девять этнических групп. Существенным результатом является также и то, что представителям ни одной нации нельзя приписать черты полностью превратного толкования этих понятий по сравнению с жителями, например, США или Великобритании [19]. Энг и Ло [20] показали, что отношение к незаконному копированию ПО определяется тремя факторами: субъективно воспринимаемым личным выигрышем (например, социальное приятие, возврат долга, благосклонность), альтруизмом и субъективно воспринимаемыми негативными последствиями – если опустить вопрос о незаконности этого действия.

Злоупотребления применением Интернета в хакерском сообществе

Помимо аттитудов, немаловажным фактором в кибер-этике считается фактор личной компетентности. Рассмотрим, к примеру, деятельность хакеров [21–23]. Эта андерграундная популяция, хотя и заметно неоднородная по характеру своих устремлений, методов, степени публичности и т.д., тем не менее обладает однородной спецификой в сфере кибер-этики. Действительно, любое изобретение, защищающее от взлома, быстро испытывается на прочность противодействующими технологиями. Несанкционированные вторжения в удаленные компьютеры и базы данных, попытки «положить» веб-сервер (denial of service), распространение вирусов происходят все чаще и чаще. Таким образом, постоянно растет квалификация и популяция хакеров; параллельно, как полагают, растет масштаб причиняемого вреда.

Существуют разные типологии компьютерных преступников. Согласно одной из них, следует проводить разграничение между следующими группами: профессиональные преступники (террористы – участники кибер-войн), преступники в белых воротничках, недовольные служащие и подростки [24, 25]. Роджерс [26] выделяет подгруппы хакеров по уровню компетентности, сферам интересов (мобильные телефоны, ПК, Интернет, кредитные карты) и характеру поведения: новички, кибер-панки, кодировщики, «старая гвардия», профессиональные пре-

ступники, пользующиеся своим знанием устройства системы служащие фирм (internals), кибер-террористы. Очевидно, что между группами нет четкой границы. В полном согласии с жизненной реальностью во все группы входят дети и подростки. Наименее квалифицированные подростки известны как «новички». Каждый день появляются «новички», которые видят в хакерстве модное хобби или выгодное занятие. «Новички» начинают с простейших заданий – просто для развлечения, далее некоторые из них обращаются к более сложным заданиям и постепенно становятся либо квалифицированными хакерами, либо профессионалами в области компьютерной безопасности; большинство же тех, кто пробует себя в этой сфере, бросают её на уровне «новичка» и, таким образом, покидают популяцию хакеров [27, 28].

Можно предположить, что огромное число актов хакерства со стороны молодежи осуществляется в силу их неспособности предвидеть последствия своих действий, а значит, и ответственности за порчу, незаконные или, по крайней мере, неэтичные поступки. Если бы «новички» досконально представляли себе вредоносные последствия своих действий, многие из них никогда бы не использовали «вандальное» ПО для взлома. Мягкие и, как правило, непреднамеренные формы правонарушений являются результатом небрежности, игрового обмана, незрелости, безразличия, недостатка любопытства или просто невежества [29]. Неосведомленность не всегда означает безразличие, невежество или недостаток любопытства; в случае детей или подростков это часто связано с психологической неспособностью перенести в новую ситуацию хорошо освоенные поведенческие механизмы. Действительно, в киберпространстве мы часто оказываемся в незнакомых, непредвиденных ситуациях; это относится как к детям и подросткам, так и к взрослым.

Новое направление в исследовании кибер-этики

Центральное положение этой статьи может быть сформулировано следующим образом. Решения некоторых новых проблем, имеющих отношение к кибер-этике, не могут базироваться исключительно на этической почве; вместо этого при принятии решений следует в полной мере учитывать данные психологии развития. Таким образом, новейшая тенденция в кибер-этике – это, на наш взгляд, ее взаимосвязь с психологией, а в дальнейшем – с практикой образования.

У любой медали имеются две стороны. Невозможность простого переноса норм этического поведения в кибер-пространство, и, таким образом, «невинные» кибер-преступления делают детей и подростков жертвами мошенников, педофилов и/или манипуляторов. Представите-

ли молодежи, бывает, «по простоте душевной» информируют незнакомых людей о сведениях личного характера – о себе или о своей семье, рискуют встречаться со взрослыми «друзьями» по Интернет-переписке, получать от них подарки, а в итоге нередко подвергаются сексуальному харассменту. Использование Интернета для общения, работы, познания и развлечений приносит новые образовательные и этические дилеммы и проблемы для родителей и учителей – проблемы в той области, в которой у воспитателей, учителей и школьных администраторов обычно недостает подготовки. Использование Интернета детьми школьного возраста ставит технические, юридические, организационные и этические (или кибер-этические) проблемы, которые в значительной степени пересекаются с собственно психологическими проблемами.

Сообществу Интернет-пользователей следует заняться обучением новых поколений основам кибер-этики. Это обучение, конечно, должно быть основано на традиционной морали и должно привносить в ИТ-среду общеизвестные нравственные нормы. Едва ли сами по себе компьютерные преступления в результате такого обучения исчезнут, однако по крайней мере приток новичков из числа новых поколений молодежи может оказаться редуцированным. Необходимо отметить, что теоретические модели этического поведения подчеркивают важность так называемой этической чувствительности, или способности отличать этическое поведение от неэтичного [30, 31]. Показано, что факторы, оказывающие влияние на различение этического и неэтичного, меняются [11]. Кроме того, способность распознавать этические выходы из ситуации и оценивать этические/неэтичные альтернативы зависит от индивидуальной системы ценностей [31].

Организационная поддержка исследований в новых областях кибер-этики

Встречаясь с новыми задачами, педагоги, эксперты в области ИТ и в области права, а также ответственные родители демонстрируют свою озабоченность и заинтересованность. Книги по этой тематике стали бестселлерами [32] – этот факт может послужить сигналом к участию в решении проблем всех заинтересованных сторон. Несколько организаций и ассоциаций (www.cybersmart.org/, www.internetwatch.org.uk/, www.staysafeonline.info, etc.) заявляют о готовности консультировать любого заинтересованного человека или группу людей по поводу новейших исследований кибер-этики. Энтузиасты разработали рекомендации по безопасному использованию детьми и подростками Интернета. Так, например, в Шотландии был запущен проект SUSI (Safer Use of

Services on the Internet – Безопасное Применение Сервисов Интернета) (www.besafeonline.org/). Наиболее амбициозным проектом является Cybercitizen Awareness Program (www.cybercitizenship.org), который поддерживается департаментом юстиции США, а также американской Ассоциацией Информационных Технологий. В рамках этой организации было проведено несколько веб-конференций. Различные правительственные ресурсы разработали множество полезных рекомендаций для детей, родителей и преподавателей (www.cybercrime.gov/rules/cyber-citizen.htm, www.usdoj.gov/criminal/cybercrime/, etc.).

В попытках гарантировать безопасность и сделать веб-навигацию для учащихся школьного возраста настолько безопасной, насколько это возможно, большинство сайтов и книг обращаются исключительно к традиционной кибер-этике. Стараясь предупредить или заблокировать непристойное/неэтичное использование Интернета, нам обычно предлагают такие меры, как усиление служб безопасности, немедленные и четкие отчеты, жесткие санкции и т.д. Но все это – лишь одна сторона медали. Другая же – минимизация того вреда, который наносят несовершеннолетние. Для этого абсолютно необходима образовательная программа: дети и подростки нуждаются в информации о возможных аморальных последствиях неконтролируемого использования информации и коммуникационных технологий. Обоснование острой необходимости и неотложности такого обучения было уже представлено и в нашей стране, однако это были пока что не более чем отдельные возгласы, не ставшие еще системой [33–36].

Новейшие образовательные аспекты

Любой старшеклассник из числа новых поколений нуждается в такой потенциальной образовательной программе. Продвинутый курс должен быть ориентирован на наиболее искушенных компьютерных/Интернет-пользователей (владельцев собственных домашних страничек, хакеров, геймеров, победителей местных или общенациональных соревнований программистов-старшеклассников и т.д.). Подобная программа должна быть интернациональной, так как в кибер-пространстве нет государственных границ. Более того, очень ограниченное количество «веб-целей» популярны среди хакеров и в основном включают сайты и веб-страницы из США (это, например, Пентагон, а также множество всемирно известных компаний, в особенности работающих в сфере ИТ). Для защиты этих «веб-целей» предпочтительно объединять средства компьютерной защиты – различные брандмауэры (firewalls) – и образовательные средства. Именно последние могут помочь в снижении

количества компьютерных «новичков» (то есть тех, кто недавно вошел в среду хакеров/крэкеров/фрикеров и т.д.).

Образовательные курсы должны быть основаны на психологических данных, описывающих стадии морального развития в детстве и отрочестве (и, конечно, во взрослом возрасте тоже). Наиболее разработанная теория, которая доказала свою ценность, была представлена Л. Кольбергом [37] и описана, в частности, в работе [38]. По Кольбергу, имеются 3 стадии – до-традиционная мораль, традиционная мораль и пост-традиционная мораль (при этом в каждой стадии есть по две под-стадии).

Маловероятно, что, тестируя суждения детей и подростков, мы обнаружим высшие стадии морального развития. Правда состоит в том, что даже многие взрослые за всю свою жизнь никогда не достигают этих высших стадий моральных суждений. Кажется также маловероятным, что тинейджеры могут быть достаточно зрелыми для того, чтобы основывать свои суждения на независимой моральной системе пост-традициональных ценностей. Легко поверить, что в онлайн большинство детей и подростков демонстрируют более низкую ступень морального развития, чем в реальной жизни. Возможное объяснение лежит в сфере анонимности Интернет-контактов. Например, очень немногие тинейджеры украдут бумажник из чужого кармана, но в то же время многие из них не считают зазорным приобретать какие-то вещи через Интернет, используя украденные номера кредитных карточек. Таким образом, главная задача состоит в том, чтобы адаптировать подростковую систему моральных суждений к условиям анонимного применения Интернета. Традиционные труды по кибер-этике не учитывают эту задачу. Новые же книги и образовательные программы с большой вероятностью встретятся с этой задачей: мы верим, что именно по этой причине кибер-этика будет пересекаться с психологией развития.

ЛИТЕРАТУРА

1. *Grodzinsky F.S.* The development of the 'ethical' ICT professional and the vision of an ethical on-line society: how far have we come and where are we going? *ACM SIGCAS Computers and Society*. 30 (1). 2000. P. 3–7.
2. *Langford D.* (ed.). *Internet Ethics*, Houndmills et al. 2000, Macmillan Press.
3. *Rotenberg M.* Protecting Human Dignity in the Digital Age, Infoethics 2000. Ethical, legal and Societal Challenges of Cyberspace. Third International Congress. UNESCO Headquarters, Paris, France, 13–15 November, 2000. Final Report and Proceedings. webworld.unesco.org/infoethics2000/report_151100.html#rotenberg
4. *Spinello R.A. & Tavani H.T.* (eds.). *Readings in CyberEthics*. 2001, Jones and Bartlett Publ.

5. *Whine M.* Far right extremists on the Internet, *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*, eds. D. Thomas & B. Loader 2000. L. & N.Y.: Routledge. P. 234–250.
6. *Buchanan E.A.* (ed.) *Readings in Virtual Research Ethics: Issues and Controversies*. Hershey, London, Melbourne, Singapore: Information Science Publishing, 2004.
7. *Frankel M.S. & Siang S.* Ethical and Legal Aspects of Human Subjects Research on the Internet: A Report of a Workshop June 10–11, 1999. American Association for the Advancement of Science (AAAS), 1999. www.aaas.org/spp/dspp/sfrr/projects/intres/report.pdf
8. *Hudson, J.M. & Bruckman A.* "Go Away": Participant Objections to Being Studied and the Ethics of Chatroom Research. *The Information Society*, 20(2), pp. 127–139, 2004.
9. *Jamal K. & Bowie N.E.* Theoretical Considerations for a Meaningful Code of Professional Ethics. *Journal of Business Ethics*. 1995. 14. P. 703–714.
10. *Rest J.R. & Narvaez D.* *Moral Development in the Professions: Psychology and Applied Ethics*, Mahwah, N.J.: Lawrence Erlbaum, 1994.
11. *Cronan T. P. & Kreie J.* Making ethical decisions. *Communications of the ACM*. 2000. 43(12). P. 66–71.
12. *Mason R.O., Mason F.M. & Culnan M.J.* *Ethics of Information Management*. Thousand Oaks, CA: Sage Publ., 1995.
13. *Panteli A.* Code Confidential: Codes of Practice for Computing Professionals. *ACM SIGCAS Computers & Society*. 2000. 32(6). www.computersandsociety.org/AccessController/sigcas/subpage/sub_page.cfm?article=844&page_number_nb=1
14. *McGuire Sh., D'Amico E., Tomlinson K. & Brown S.* Teenagers self-reported motivations for participating in computer crime, 8th International Conference on Motivation (Workshop on Achievement and Task Motivation). Abstracts. Moscow, 2000. P. 72–73.
15. *Ruf B.M. & Thomas S.B.* Unethical decision-making with computer usage in a university environment, 2003. <http://aaahq.org/AM2003/EthicsSymposium/Session%205a3.pdf>
16. *Debnath N. & Bhal K.T.* Religious belief and pragmatic ethical framework as predictors of ethical behavior, eds. F. Sudweeks & Ch. Ess, *Cultural Attitudes towards Technology and Communication*. Proceedings of the 3rd International Conference (Montreal, Canada, 12–15 July, 2002), 2000. P. 409–420.
17. *Kim K.H.* A study of the conduct of Korean IT participants in ethical decision making, eds. C.-H. Chung, C.-K. Kim, W. Kim, T.-W. Ling & K.-H. Song, *Web and Communication Technologies and Internet-Related Social Issues – HSI 2003*. Proc., Second International Conference on Human Society@Internet (Seoul, Korea, June 2003). *Lecture Notes in Computer Science*, 2713, Berlin et al.: Springer. 2000. P. 64–74.
18. *Voiskounsky A.E., Babaeva J.D. & Smyslova O.V.* Attitudes towards computer hacking in Russia, eds. D. Thomas & B. Loader, *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*, L. & N.Y.: Routledge, 2000. P. 56–84.
19. *Whitman M.E., Townsend A.M. & Hendrickson A.R.* Cross-national differences in computer-use ethics: A nine-country study. *Journal of International Business Studies*, 30(4), 1999. P. 673–687. http://copenhagen.jibs.net/Archive/1999/30_4_99_673.pdf
20. *Ang A.Y. & Lo B.W.N.* Software piracy attitudes of tertiary students in Australia, 2001. www.hkcs.org.hk/search/cced/ed11_aa.htm
21. *Войскунский А.Е., Петренко В.Ф., Смылова О.В.* Мотивация хакеров: психосемантическое исследование // *Психологический журнал*. 2003. Т. 24, № 1. С. 104–118.
22. *Sterling, B.* *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. London: Penguin, 1992.
23. *Taylor P.* *Hackers*. Crime in the Digital Sublime, London: Routledge, 2002.
24. *Nicholson L.J., Shebar T.F. & Weinberg M.R.* Computer crimes. *American Criminal Law Review*, 2000. www.albany.edu/acc/courses/acc680.spring2001/curtin101.ppt

25. *Shinder D.L. & Tittel E.* Scene of the Cybercrime: Computer Forensics Handbook, Syngress Media Inc., 2002.
26. *Rodgers M.* A new hackers' taxonomy, Dept. of Psychology, University of Manitoba, 1999. www.mts.net/~mkr/hacker.doc
27. *Войскунский А.Е., Смылова О.В.* Роль мотивации потока в развитии компетентности хакера // Вопросы психологии. 2003. № 4. С. 35–43.
28. *Voiskounsky A.E. & Smylova O.V.* Flow-Based Model of Computer Hackers' Motivation. *CyberPsychology & Behavior*. 2003. 6(3). P. 171–180.
29. *Suler J.R. & Phillips W.* The Bad Boys of Cyberspace: Deviant Behavior in Multimedia Chat Communities. *CyberPsychology and Behavior*. 1998. 1. P. 275–294. www.rider.edu/~suler/psycyber/badboys.html
30. *Bommer M., Gratto C., Gravander J., & Tuttle M.* A Behavioral Model of Ethical and Unethical Decision Making // *Journal of Business Ethics*. 1987. 6. P. 265–280.
31. *Wortuba T.R.* A Comprehensive Framework for the Analysis of Ethical Behavior, with a Focus on Sales Organizations // *Journal of Personal Selling and Sales Management*. 1990. 10(1). P. 29–42.
32. *Schwartau W.* Internet & Computer Ethics for Kids (and Parents&Teachers Who Havent Got a Clue), Inter-Pact, 2001.
33. *Бабаева Ю.Д., Войскунский А.Е.* Одаренный ребенок за компьютером. М.: Сканрус, 2003.
34. *Бондаренко С.В.* Киберэтика и сетевые сообщества (молодежный аспект проблемы, с точки зрения американских социологов и психологов) // Социальные и психологические последствия применения информационных технологий: Мат-лы международной Интернет-конференции / Под ред. А.Е. Войскунского. М., 2001. С. 243–252.
35. *Бондаренко С.В.* Социальная структура виртуальных сетевых сообществ. Ростов н/Д., 2004.
36. *Войскунский А.Е.* Психологическая характеристика потенциально негативных последствий применения компьютерных технологий // Молодежь в компьютерно-игровых и интернет-центрах: Сборник методических материалов (по итогам работы круглого стола). М.: АРКЦентр, 2004. С. 33–37.
37. *Kohlberg L.* The Meaning and Measurement of Moral Development. Clark Univ. Press, 1981.
38. *Анцыферова Л.И.* Связь морального сознания с нравственным поведением человека (по материалам исследований Лоуренса Колберга и его школы) // Психологический журнал, 1999. Т. 20, № 3. С. 5–17.