УДК: 004.056.5

СОЦИАЛЬНО-ФИЛОСОФСКИЕ АСПЕКТЫ ЦИФРОВОГО ВТОРЖЕНИЯ

SOCIAL AND PHILOSOPHICAL ASPECTS OF THE DIGITAL INVASION

О.М. Манжуева
O.M. Manzhueva

Восточно-Сибирский государственный институт культуры, Россия, 670031, г. Улан-Удэ, ул. Терешковой , 1
East-Siberian State Institute of Culture, 1 Tereshkova St, Ulan-Ude, 670031, Russia

E-mail: ocydenova@yandex.ru

Аннотация: В статье рассмотрены социально-философские аспекты хакерской деятельности в глобальной сети. Отражены взгляды компьютерной этики на решение проблем безопасности информации в информационном пространстве.

Resume: Ethical aspects of hacking use consider in this article. There were revealed the views of computer ethics on information security issues in the information space.

Ключевые слова: информационная безопасность, информационное взаимодействие, защита информации, компьютерная этика, хакерские атаки.

Key words: information security, information interaction, information security, computer ethics, hacker attacks.

Сегодня под словосочетанием «компьютерная этика» подразумевается направление прикладной этики, изучающее социальное и этическое действие информационных технологий на все области общественной жизни. Данное направление рассматривает влияние информационных технологий на ценности человека, используя концепции, теории, процедуры из философии, социологии, права, психологии и т. д. Независимо от данного ей определения или взглядов на ее уникальность, лучшим способом представить природу компьютерной этики поможет анализ исследуемых ею вопросов посредством репрезентативных примеров животрепещущих проблем.

Вопросы обеспечения защиты информации от угроз и опасностей искусственного характера находят свое яркое отражение в области компьютерной этики. В эпоху компьютерных вирусов философы, понимая актуальность данной проблемы, в разделе компьютерных преступлений особое внимание уделяют такой теме, как противоправные действия хакеров. Например, по мнению Т. Байнама, наболевшую проблему информационной безопасности представляют действия хакеров [1, с. 7], функции которых состоят в незаконном проникновении в автоматизированные информационные системы. В подобном случае действия хакеров обычно подразделяются на намеренно совершаемый вандализм и кражу различного характера данных, и действия, совершаемые под руководством исключительно интереса, с целью «исследования» компьютерной системы. Эти «исследователи» позиционируют себя как благожелательные защитники устойчивости информационной среды и апологеты борьбы с мошенничеством в корпорациях или шпионажем национальных агентов. Так, самоназванные участники «комитета бдительности» утверждают, что не оказывают вреда, но несут пользу информационному обществу, выявляя неблагонадежные элементы. В то же время, необходимо признать, что всякая акция хакера неизбежно наносит ущерб, потому что заставляет владельца компьютерной системы провести детальный контроль на наличие поврежденных программ или потерю данных. В том случае, даже если взломщик не произвел изменений в системе, потерпевшая сторона обязана осуществить осмотр компьютерной системы.

В свой черед, К. Химма к кибератакам относит нарушения целостности информации без преднамеренного умысла дезорганизовать работу системы, например, из-за любопытства, равно как из-за желания незаконным путем завладеть конфиденциальной информацией в целях личной выгоды, финансового обогащения, вымогательства и т. д. Исследователь внимательно рассматривает этические проблемы каждой из сторон киберконфликта [2]. К. Химма изучает философию деятельности хакера и его этические принципы, заложенные в основе действий, рассматривая «за» и «против» цифрового вторжения. Так он отмечает, что равенство и демократия стали, возможно, спонтанно, но определяющими свойствами сети Интернет, задающими новое, свободно организованное, политическое измерение. Такое либеральное проявление равенства устанавливает одинаковые альтернативы в цифровой реальности вне зависимости от пола, физических возможностей организма, этнической принадлежности, религии и т. д. Философия хакеров отличается яркими либеральными принципами, отражающимися в этических максимах, определяющих действия

этой социальной группы. В практике имеются конкретные случаи, когда хакерское сообщества внесло свою лепту в законодательные процессы, оказавшие действительно решающее значение в дебатах о свободе слова и цензуре в среде Интернет.

Кроме того, К. Химма отмечает исключительную специфику Интернет, оказавшую революционное влияние на содержание таких понятий, как работа и досуг. Интернет заложил основу новому подходу к работе, сокрушая привычное восприятие времени. Использование новой технологии позволяет изменять границы работы и отдыха в информационном обществе, в результате чего хакерскую этику причисляют к новой трудовой этике, которая бросает вызов протестантскому смыслу, вложенному в слово «работа». Из его поля зрения не ускользают даже возможные положительные социальные эффекты от «доброкачественного вторжения» хакеров, проливающие свет на уязвимые места систем защиты. Также он не оставляет без внимания роль государства в обеспечении защиты от действий хакеров. В результате приходит к выводу: независимо от того, что цифровое вторжение не нарушает физическое пространство человека, но несет потерю конфиденциальности его информационного содержания в компьютере, соответственно морально оправдано быть не может. Что же касается роли государства, то в данный момент правоохранительные органы не имеют необходимых ресурсов для обеспечения минимальной защиты от действий хакеров, отчего решение проблем от цифровых нападений всецело ложится на плечи собственников информации. Здесь он употребляет такое понятие, как «этика киберзащиты», служащая моральным оправданием действий последних в процессе защиты собственных информационных ресурсов.

Исследуя проблемы обеспечения безопасности в компьютерных системах, Р. Шульц, в свою очередь, приходит к выводу, что безопасность всегда предполагает некий компромисс: предотвращение нежелательного доступа посторонних лиц к некоторым ресурсам ведет к усложнению доступа самого собственника. Это правило включает любую функцию безопасности. По его мнению, «безопасности только ради безопасности» не несет смысла. При этом он приводит пример, ярко демонстрирующий все стороны указанного компромисса: «ключ к моей машине не позволяет другим, превратить ее в движущую силу, но я должен быть осторожным, чтобы не потерять этот ключ. Кроме того, сам по себе ключ является механизмом, который вполне может стать неисправным» [3, с. 46]. Этим самым Р. Шульц говорит о том, что в основе безопасности лежит постоянная работа, заключающаяся в бдительном контроле и в определенных затратах финансового и административного характера.

Здесь необходимо подчеркнуть важную мысль: философы не ставят цель найти конкретные ответы на вопросы указанных проблем, они предлагают этические рамки, в которых возможно принять решение, используют примеры для иллюстрации, принципы и механизмы. Эксперты в области компьютерной этики не предпринимают попыток достичь окончательного этического решения, поскольку, по их мнению, для этого требуется гораздо более тщательный анализ поведения нарушителя и характер конкретной кибератаки, а также контекст, в котором она проводится.

Одно из направлений компьютерной этики рассматривает проблемы компьютерной безопасности через призму гендерных характеристик. В противовес многим концепциям о торжествующем равноправии в информационной среде, данное течение исследуют вопросы о роли гендерных характеристик в процессе обеспечения безопасности и решения проблем использования информационной технологии. Подобный подход ввел в 1990 году понятие «киберфименизма», предполагающего свои решения в изучении этических проблем в процессах использования технологий современного общества. Киберфеминизм предполагает течение в философской и литературной мысли, обращенное к исследованию и популяризации основных постулатов киберкультуры, берущей начало в 1980-е годы на подъеме интереса к изучению новых технологий в таких областях, как технологии виртуальной реальности, кибернетика и биомедицина. В границах компьютерной этики данное направление пытается найти ответы на следующие вопросы: Какую роль в формировании профессионалов в области информационных технологий играют гендерные характеристики? Оказывает ли гендерный фактор влияние на развитие киберпреступности? и т. д. В свою очередь, приверженцы указанного подхода преследуют цель выйти за границы только феминистского желания пошатнуть мужской контроль управления информационными технологиями, но решить моральные, правовые, политические и социальные проблемы.

Принято считать, что численность профессионалов, занятых в сфере информационных технологий, неоспоримо ведет к преобладающему количеству специалистов среди мужчин, также как и статистика расследования преступлений в информационной среде отражает преобладающее число хакеров мужского пола [4, с. 18]. Исследование виртуального игрового мира еще раз подтвердило проблему гендерного неравенства. Проведенный Интернет-обзор игр показал доминирующее число мужских персонажей, которое связывают, прежде всего, с ориентированностью геймплея на мужской стиль игры, что ведет к потенциальному отчуждению женщин игроков [5, с. 158]. При этом Д. МакМахон и Р. Коэн отмечают явную связь пола с принятием этических решений в виртуальном онлайновом мире [6, с. 8]. Согласно результатам их исследования, женщины чаще задумываются об этичности поступков, нежели мужчины.

Относительно поиска неуловимых хакеров-женщин существует несколько предположений. Одно из них, как результат эмпирического исследования, связывает низкое число хакеров-

женщин на фоне общего количества киберпреступников с параллельно низким числом женщин, занятых в области информационных технологий [7]. Следующая группа ученых, базируясь на философии полов, описывает это явление следующим образом. Женщины более консервативны в своих суждениях, поэтому применение этических мер безопасности по отношению к ним на уровне внушения будет достаточным, тогда как мужчины способны потребовать более существенных сдерживающих механизмов, регулирующих поведение в информационной среде [8].

Основатель теории хакерской этики С. Леви следующим образом описывает хакеров: «со стороны кажется, что хакеры ведут странные разговоры, у них не стандартный распорядок дня, они едят странную пищу, и они все свое время думают о компьютерах» [9, с. 173]. Анализируя признаки зависимости от Интернет-сеансов, он констатирует: к проблемам, связанным с гигиеной, женщины относятся сложнее, нежели мужчины, и это может быть достаточным основанием для уменьшения числа хакеров среди женщин. Кроме того, биологические и социальные функции, предначертанные в женщине, изначально устраняют ее из сообщества хакеров [10]. В силу присущей ей ответственности за уходом и заботой о детях, доме, женское представление о работе и досуге существенно отличается от мужского. Коммуникационные технологии и сеть Интернет воспроизводят стандартные гендерные модели, предполагающие наличие свободного времени. «Трудясь в две смены – на оплачиваемой работе и дома» [11, с. 80], женщина не всегда располагает возможностью посвятить ночное время хакерской деятельности, более того, компьютер не может выполнять работу по уходу за ребенком и семьей в реальной жизни.

Так, основные направления киберфеминизма относятся к социально-философскому анализу информационной технологии и роли женщины в ходе ее применения. Целью исследований данной концепции служит борьба со сложившимися представлениями о мужском контроле технологии, в частности новых информационных технологий, достижения равноправия женщин и мужчин в процессах их использования, иначе, своего рода некритический энтузиазм в области науки, техники и прав женщин. В свою очередь, описанная концепция подвергается значительной критике, характеризуется утопической. Нет мужского или женского хактивизма. Хакеров характеризуют результаты их деятельности, а не принадлежность к определенной расе, религии или полу, убежден С. Леви [9, с. 378].

В то же время, сторонники данного течения отмечают положительные аспекты идеи киберфеминизма. Исследователи выделяют, что феминистская этика отличается особой практичностью, предугадывая в данном факте начало альтернативной феминистской технонауки, дающей новую трактовку некоторых социально-философских аспектов в области информационной безопасности. Дело в том, что социальные и политические позиции женщин, поддерживающих идеи киберфеминизма, предлагают альтернативные взгляды на хакерскую активность. Существует ряд доказательств, что женская хакерская этика может отличаться от мужских подходов в хакерской деятельности, например, в отношении таких аспектов, как свобода слова, дискриминация, защита прав детей. Порой проявления альтернативного движения феминистской хакерской этики в сохранение общепринятых идеалов, резко расходятся с продекларированными хакерскими принципами свободы слова в сети. Примером того может служить «крестовый поход против порнографии в Интернет», в рамках которого женщины-хакеры использовали свои навыки, чтобы обнаружить интернет-сайты, специализирующиеся на распространении детской порнографии, с целью передать информацию в правоохранительные органы.

Важно заметить, авторы подхода не ставят цель доказать статистку. Они анализируют общий вклад феминистской версии компьютерной этики в борьбу за права человека информационного века и защиту идеалов общества, в надежде вызвать интерес к подходу гендерного анализа, проливающего свет на новые решения этических проблем современного общества, и дальнейшего направления его научного развития.

Таким образом, в рамках исследования обеспечения безопасности, компьютерная этика представляет особый интерес, поскольку изучает такое основообразующее понятие в данной области, как безопасность информации, выраженную в защите конфиденциальности, целостности и доступности. Несмотря на тот факт, что урегулирование поднятых вопросов, как принято считать, находится в большей степени в юрисдикции законодательства государственных органов, специалисты по компьютерной этике предлагают собственные пути формирования более универсальных оснований для определения справедливости и общего морального блага в границах концепции информационной безопасности. Так, в рамках социально-философских исследований, они изучают особенности среды Интернет, создавшей почву для осуществления логических атак на компьютерную безопасность, философию участников информационного взаимодействия и факторы, влияющие на процесс обеспечения защиты информации. Философы предлагают этические рамки, которые наиболее благоприятны, по их мнению, для решения проблемы обеспечения безопасности информации, при этом требуя более тщательного анализа поведения каждого характера и конкретной кибератаки, а также контекст, в котором она проводилась.

Список литературы
References

1. Bynum T. The Foundation of Computer Ethics // Computers and Society, 2000. – № 30(2). – P. 6–13.
2. Himma K. Ethical Issues Involving Computer Security: Hacking, Hacktivism, and Counterhacking / The handbook of information and computer ethics. – New Jersey: Wiley-Interscience, 2008. – 704 p.
3. Schultz R. Contemporary issues in ethics and information technology. – Hershey: IRM Press (an imprint of Idea Group Inc.), 2006. – 144 p.
4. Adam A. The Gender Agenda in Computer Ethics //Computers and Society, 2000. – № 30(4) – P.17–24.
5. Soukup C. Mastering the Game: Gender and the Entelechial Motivational System of Video Games // Women's Studies in Communication, 2007. – Vol. 30(2). – P. 157–178.
6. McMahon J., Cohen R. Lost in cyberspace: ethical decision making in the online environment // Ethics and Information technology, 2009. – Vol. 11(1). – P. 1–17.
7. Taylor P. Hackers: Crime in the Digital Sublime. – London and New York: Routledge, 1999. – 134 p.
8. Kreie J., Cronan T. How men and women view ethics // Communications of the ACM, 1998. – № 41(9). – P. 70–76.
9. Levy S. Hackers. Heroes of the Computer Revolution. – New York: Doubleday, 1984. – 337 p.
10. Adam A., Green E. On-line leisure: gender and ICTs in the home // Information, Communication and Society, 1998. – № 1(3). – P. 291–312.
11. Cudd A. Objectivity and ethno-feminist critiques of science /After the Science Wars. – New York and London: Routledge, 2001. – P. 92–94.