О. Б. СКОРОДУМОВА

ХАКЕРЫ КАК ФЕНОМЕН ИНФОРМАЦИОННОГО ПРОСТРАНСТВА

СКОРОДУМОВА Ольга Борисовна - кандидат философских наук, доцент кафедры культурологии Московского гуманитарного университета.

Актуальность и разработанность проблемы

Интенсивное развитие современного общества в России приводит к широкому распространению новых информационных технологий в различных социальных слоях общества. По данным департамента регулирования предпринимательской деятельности и корпоративного управления Министерства экономического развития и торговли РФ доступ к Интернет в 2003 г. имели 8,5 млн. пользователей, из которых 35% осуществляли его с личных компьютеров; 45% - с компьютеров предприятия; 20% - из публичных, государственных учреждений. К 2005-2006 г. их число увеличится

в 2,3 раза и достигнет 20 млн. В 2006 г. в каждой городской школе должны быть 1-2 компьютерных класса и в сельской - не менее 5 компьютеров. Эти прогнозы опираются на ряд стратегических правительственных документов, которые в начале нового столетия разработаны и утверждены в нашей стране. Среди них: "Концепция формирования информационного общества в России", "Доктрина информационной безопасности Российской Федерации", "Концепции формирования и развития единого информационного пространства России", долгосрочные Федеральные целевые программы: "Электронная Россия (2002-2010 гг.)", "Развитие единой образовательной информационной среды (2001-2005 гг.)", городские программы "Электронная Москва" и "Электронный Санкт-Петербург".

Успешная реализация данных программ предполагает разработку стратегии по обеспечению информационной безопасности и снижению компьютерной преступности. Важнейшим фактором реализации данной задачи становятся комплексные гуманитарные исследования, предполагающие анализ социокультурных факторов компьютерной преступности. В документе "Приоритетные проблемы научных исследований в области информационной безопасности Российской Федерации", принятом Советом безопасности РФ в 2001 г., особое внимание уделяется гуманитарным аспектам данной проблемы. Подчеркивается, что важнейшим условием решения поставленных задач являются: ценностная ориентация, информационное обеспечение, информационно-психологическая безопасность личности и общества [1].

В данной статье исследуется один из важных аспектов обеспечения информационной безопасности - борьба с хакерами, рассматриваются истоки хакерства, противоречивость оценок этого феномена, выявляются характер и сущность трансформаций хакерской субкультуры, опираясь как на собственные манифестации хакеров, так и на данные исследований статистики компьютерных преступлений в нашей стране и за рубежом.

В исследованиях деятельности хакеров доминируют два подхода. Первый из них на основе критерия несанкционированного вторжения в информационную систему отождествляет хакерство с преступной деятельностью. Наиболее распространен среди представителей структур госбезопасности. Опираясь на данный критерий, проводится классификация деятельности хакеров. Например, в разработанной на факультете информационной безопасности МИФИ [2] выделяются:

"шутники" - осуществляют взлом компьютерной системы для достижения известности. Не склонны причинять серьезного вреда системе и выражают себя внесением различных юмористических заставок, вирусов с различными визуально-звуковыми эффектами (музыка, дрожание или переворачивание экрана, рисование всевозможных картинок и т.п.);

"фракеры" - осуществляют взлом интрасети в познавательных целях для получения информации о топологии сетей, используемых в них программно-аппаратных средствах и информационных ресурсах, а также реализованных методах защиты;

"взломщики-профессионалы" — осуществляют взлом компьютерной системы с целями кражи или подмены хранящейся там информации. Для них характерна системность и организованность действий (исследование вычислительной системы с выявлением изъянов в ней, разработка программной реализации атаки и непосредственное ее осуществление). Разновидностью этой категории хакеров являются взломщики программного обеспечения и специалисты по подбору паролей;

"вандалы" - осуществляют взлом компьютерной системы для ее разрушения: порча и удаление данных, создание вирусов или "троянских коней".

Второй подход опирается на критерий мотивации при оценке деятельности хакеров: "человек, подсматривающий и ищущий (хакер) становится взломщиком, действующим корыстно (кракер), беспредельно разрушительно (кибертеррорист) или идейно (хактивист)" [3].

В среде технической интеллигенции, связанной с информационными технологиями, сформировался третий подход. "Хакерство" рассматривается как исторический и

социокультурный феномен, имеющий собственные специфические признаки на различных этапах своего развития. Анализу разных этапов хакерского мировоззрения и практики посвящен целый ряд работ зарубежных и отечественных исследователей (Касперски К., Леви С, Тайли Эд, Bruce Sterling, Медведовский И.Д. и др.) [4], [5], [6], [7], [8]. Но в основном наиболее активно освещение сущности и особенностей этого явления ведется на хакерских сайтах и порталах, где даются самооценки, раскрываются собственные идеи, ценности и образ жизни [9]. Хакеры достаточно активны в обнародовании своих принципов, взглядов и представлений. Они имеют разветвленную систему сайтов и порталов, электронных журналов, проводят конференции и съезды в национальном и международном масштабе. Подобного рода активность приводит к формированию сленга [10], складываются традиции обмена опытом, в том числе и идейным, отражаемым в научной и художественной публицистике. В монографических исследованиях, посвященных субкультуре хакеров, в силу популярности темы и широкого коммерческого спроса преобладает описательный подход, ориентированный на широкую аудиторию [11].

Рост популярности хакеров и романтизация их образа жизни при отсутствии целенаправленной просветительско-правовой и воспитательной работы представляет значительную опасность. Этому во многом способствует привлечение наиболее известных из них на высокооплачиваемую работу в солидные компании мира. Так, например, крупнейший взломщик Кевин Поулсен сразу же после выхода из тюрьмы был приглашен на работу в известную телевизионную компанию "Tech TV", для сайта которой он освещал события из мира компьютерной безопасности. Сейчас Кевин - редактор известного Интернет-журнала "SecurityFocus" (Фокус Безопасности - www. securityfocus.com). Многие из них, например, Джеф Мосс, становятся управляющими по проверке систем безопасности. Он же руководит отделом информационной безопасности компании "Secure Computing". По популярности видные хакеры конкурируют со знаменитыми писателями, учеными, кинозвездами: их приглашают на конференции, у них берут интервью.

Романтизация образов хакеров затронула и научные круги. В секторе информационных технологий Челябинской областной универсальной научной библиотеки открылась выставка "Хакеры - гении или злодеи?". В экспозиции представлены материалы, рассказывающие о новых преступниках XX-XXI в. - компьютерных взломщиках. Один из ведущих американских консорциумов "Ad Cops", задачей которого является борьба с мошенниками в Интернете, открыл на своем сайте (http://www.adcops.com) ресурс, посвященный обману с использованием новых информационных технологий. В виртуальном музее работает 13 тематических выставок, но вход - платный: без регистрации можно посмотреть только часть экспозиции, которая посвящена теории и практике самых разнообразных интернет-мошенничеств. Интерес к аналогичным проектам характерен и для России. Крупнейший образовательный каталог лучших Интернет-ресурсов "MUSEUM.RU" не только дает ссылку на русскоязычный "Виртуальный музей мошенничества", но и комментирует содержание его экспонатов следующим образом: "Музей рассказывает о разных способах мошенничества, надувательства и обмана, которыми не брезгуют иные фирмы. Музей поучителен, интересен, и, что самое грустное, - неизвестен" (http://www.museum.ru/museum/swindler).

Хотя и выставка, и музеи в своих декларациях заявляют о важности обобщения методик хакеров для разработки систем информационной безопасности, пристальное внимание к ним способствует созданию романтического ореола гениальности, избранности, что, несомненно, привлекает молодежь. Требуются значительные как пропагандистские усилия, так и финансовые вложения, чтобы снизить, или, по крайне мере, приостановить рост компьютерной преступности. Различные ведомства, начиная с Агентства национальной безопасности (АНБ) США и НАТО, принимают меры по защите информации, вкладывая немалые средства. Если в 2000 г. привлечено 176 млн. долл., то по оценкам аналитической компании "The Yankee Group" объем рынка услуг по обеспечению сетевой безопасности к 2005 году достигнет 2.6 млрд. долл. Необходима

и целенаправленная культурная политика: создание Интернет-сообществ, порталов, сайтов, борющихся с анархистскими взглядами, разъясняющими правовую ответственность, развенчивающих "хакерскую романтику".

Исследование хакерства имеет, с одной стороны, ряд преимуществ, а с другой - сталкивается с серьезными проблемами. К преимуществам можно отнести то, что данный социокультурный феномен, отличающийся собственным ценнностным строем, обычаями и нормами, существует уже несколько десятилетий, и накоплен значительный эмпирический материал. Становление хакерской субкультуры осуществляется параллельно с формированием глобальной Сети Интернет. Вместе с тем при исследовании данного феномена существует ряд трудностей: отсутствие возможности анализа на материале анкетирования, опросов и т.п., анонимность предоставляемых в Интернете свидетельств, лозунгов и др.

Социокультурные истоки и трансформации хакерской субкультуры

Термин "хакер" (Hacker) - пользователь, осуществляющий действия, направленные на несанкционированное использование программного обеспечения или данных, имеет этимологические корни, никак не связанные с преступной деятельностью: "хакер" - тот, кто делает мебель топором, связан с нестандартным действием, оригинальным поиском, творческим преодолением ограничений. Применительно к информационным технологиям термин "хак" (hack) означал оригинальный ход в программировании или использовании программного обеспечения, в результате которого компьютер позволял осуществлять операции, ранее не предусмотренные или считавшиеся невозможными. Тех, кто мог осуществить данную задачу, стали называть "хакерами", а пользователи, которые не могли овладеть даже предписанными действиями и не стремились к исследованию системы, получили название "ламеры" (от англ. "lamer" - неполноценный, убогий, калека).

В развитии субкультуры хакеров можно выделить ряд этапов с собственными ценностными ориентирами и характерными чертами мировоззрения.

Первый (60-е г. XX в.) - характерен установками на новаторский подход к исследованию программ, провозглашением принципа неограниченного бесплатного доступа для всех к информации, ценностей абсолютной свободы. На начальном этапе развития глобальной сети Интернет хакерское движение не носило деструктивного характера, отражая тенденцию творческого новаторства, исследования пределов систем, их потенциальных возможностей. Экспериментирование не преследовало достижения корыстных целей или нанесения ущерба. Для сообщества хакеров этого периода, куда входили студенты и профессора крупнейших университетов и научно-исследовательских центров США, характерен дух взаимного сотрудничества, демократизм, собственный четко обоснованный этический кодекс. Важнейшая особенность субкультуры хакеров на данном этапе - представление о собственной избранности, элитарности. Многие из них оценивали себя как первопроходцев, создающих новое общество, основанное на ценностях глобального киберпространства. Обращаясь к правительствам мира, один из известнейших идеологов хакеров Джон Барлоу, подчеркивая данный аспект, писал: "Правительства Индустриального мира, вы - утомленные гиганты из плоти и стали; моя же Родина - Киберпространство, новый дом Сознания. От имени будущего я прошу вас, у которых все в прошлом, - оставьте нас в покое. Вы лишние среди нас... Мы творим мир, в который могут войти все без привилегий и дискриминации, независимо от цвета кожи, экономической или военной мощи и места рождения. Мы творим мир, где кто угодно и где угодно может высказывать свои мнения, какими бы экстравагантными они ни были, не испытывая страха, что его или ее принудят к молчанию или согласию с мнением большинства. Ваши правовые понятия собственности, выражения личности, передвижения и контексты к нам неприложимы... Мы

сотворим в Киберпространстве цивилизацию Сознания. Пусть она будет более человечной и честной, чем мир, который создали до того ваши правительства" [12].

В основе идеологических и этических требований хакеров раннего периода лежали следующие принципы: свободный и неограниченный доступ к компьютерам и любой информации; полный демократизм (отрицание доверия к любым авторитетам), децентрализованность как абсолютное кредо; отрицание возможности использования критериев возраста, образования, национальной и расовой принадлежности, социального статуса при оценке человека, значимыми являются только результаты его деятельности; вера в гармонию, красоту, бескорыстность и неограниченные возможности нового виртуального мира.

Второй этап (конец 70-х гг. - начало 80-х гг. XX в.) - переход от новаторского исследования к несанкционированному вторжению в чужие системы, повышение агрессивности, использование знаний в целях протеста, удаление или изменение важных данных, распространение компьютерных вирусов и т.п. Для обозначения этой категории хакеров используется термин "кракер" (от англ. "cracker" - взломщик) - лицо, изучающее систему с целью ее взлома. Именно кракеры реализуют свои криминальные наклонности в похищении информации и написании разрушающего программного обеспечения. Они применяют различные способы атак на компьютерную систему, используя принципы построения протоколов сетевого обмена. Техническими и социально-экономическими причинами являлись: доступность компьютера широкому кругу лиц, в том числе и программистам-любителям; ужесточение конкуренции среди компьютерных фирм; машинная и программная несовместимость, ведущая к объективной потребности во взломе и доработке программ; повышенное внимание средств массовой информации к фактам взлома систем и создание ореола "героя" вокруг взломщика. Сообщество хакеров этого периода в отличие от предшественников не имеет единой мировоззренческой концепции. Выделяются различные подгруппы (они охарактеризованы в начале статьи - "шутники", "фракеры", "взломщики-профессионалы", "вандалы"), отличающиеся различными идеологическими и психологическими установками.

Третий этап (80-90-е гг. XX в.) - стремление к созданию организованных структур, сращивание хакерской субкультуры с криминальным миром.

В этот период хакерское движение становится мощной силой, способной дестабилизировать общественные структуры, превращается в один из объектов изучения государственными органами и международными правозащитными организациями. В 1979 г. на Конференции американской ассоциации адвокатов в Далласе впервые был определен состав компьютерных преступлений. Комитет министров Европейского Совета в 1989 году согласовал и утвердил "Минимальный список нарушений", рекомендованный странам-участницам ЕС для создания единой уголовной стратегии по разработке законодательства, связанного с компьютерными преступлениями, включающий: компьютерное мошенничество, подделку компьютерной информации, повреждение данных или программ ЭВМ, компьютерный саботаж, несанкционированное вторжение в систему (доступ, перехват данных, использование защищенных компьютерных программ, воспроизведение схем). В ФБР была разработана "Матрица компьютерных преступников", описывающая их обобщенные типы по категориям правонарушителей с указанием организационных, рабочих, поведенческих, ресурсных характеристик. В 1991 г. по решению 19-й Европейской региональной конференции Интерпола при Генеральном Секретариате из специалистов 16 европейских стран создана рабочая группа по компьютерным преступлениям. В России в 1997 г. для борьбы с компьютерной преступностью при МВД создано Управление "Р".

В 90-е гг. формируется новый образ хакерской (кракерской) субкультуры, для которого характерны: выраженный интерес к новинкам компьютерной техники, устройствам связи и программным средствам. Системная подготовка взлома, широкое использование агентурных и оперативно-технических методов, предварительная апробация системы методов взлома и предельно быстрое осуществление атаки, исключающее

возможность зафиксировать факт ее осуществления и принятие контрмер по отражению, выявлению личности и местонахождения атакующего типичны для хакеров нового поколения. Они точно рассчитывают рациональность методов взлома защиты компьютерной системы, разрабатывают программы действий, обеспечивающих анонимность атаки, никогда не действуя под собственным именем и тщательно скрывая свой сетевой адрес. Мировоззренческое обоснование взлома - отличительная черта хакеров этого периода. Наиболее распространенными становятся следующие виды атак: на системы управления базами данных, на операционные системы и сетевое программное обеспечение.

Хакеры широко применяют методы социальной инженерии, уделяя повышенное внимание манипулированию людьми и созданию программируемой модели поведения человека, о чем свидетельствует "Обмен опытом" на хакерских сайтах [13]. Они используют и целенаправленно формируют факторы, способные привести к сознательному или неумышленному соучастию в разрушении систем информационной защиты организации: неудовлетворенность сотрудника (сотрудников) социальным статусом или материальным положением; формирование политико-идеологических, нравственных, религиозных, бытовых ориентаций, противоречащих установкам фирмы; создание экстремальных ситуаций на личностном (семейном, сексуальном, финансовом и т.д.) уровне; давление на субъекта путем шантажа или обмана; имитацию ранговых различий с целью получения необходимой информации; воздействие на психофизические и физиологические системы организма с использованием гипноза, психотропных препаратов, наркотиков и т.п.

Четвертый этап (конец 90-х г. XX в. - начало XXI в.) - институализация хакеров: создание крупных объединений, союзов, фирм, тесным образом сотрудничающих с криминальными и теневыми структурами, активная пропаганда ценностей и принципов хакерской субкультуры через средства массовой информации.

В XXI в. интенсифицируется процесс институализации хакеров, хотя они по-прежнему строго соблюдают принцип анонимности (вместо собственного имени используются псевдонимы типа "Ludichrist", "Sicko", "Packet Rat" и др.). Создаются регулярно действующие сообщества хакеров, они имеют свои сайты, журналы: "Access All Areas" ("Вседоступность"); "Crypt NewsLetter's Home Page" ("Популярные криптографические новости"); "Old and New Hackers" ("Старые и новые хакеры"); "Chaos Computer Club" ("Клуб компьютерного хаоса"). Из отечественных: "Hacker rings" ("Кольца хакеров"), "Hackzone" ("Зона хакеров"), "Хакер" и др.

Наиболее крупные из них регулярно проводят хакерские съезды. Функционирует ежегодная конференция в Лас-Вегасе, где собираются несколько тысяч участников из многих стран мира - от США до Австралии. С 1989 г. раз в четыре года проходит представительный хакерский форум в Голландии "Hackers At Large" ("Все хакеры"). Ежегодно в Германии проходит Всемирный конгресс хакеров под эгидой "Chaos Computer Club" ("Клуб компьютерного хаоса - CCC"). "CCC" - это трехдневная конференция, посвященная технологиям, обществу и будущему человечества. В 2000 г. в Москве прошел фестиваль русских хакеров России и близлежащих стран - "СПРЫГ-2к". По сравнению с первым "СПРЫГом", проходившим в 1993 г., заметно возросло число участников конгресса: несколько десятков против 15 в прошлом. "Спрыги" приобрели статус ежегодных конференций (СПРЫГ-Ш - 2001 г.; СПРЫГ-2002; СПРЫГ-2003), их деятельность освещается на специализированном сайте "SPRYG" (http://en.spryg.zork.net).

На международных съездах хакеров отчетливо прослеживается тенденция взаимодействия хакерского движения с государственными и коммерческими структурами. В них принимают участие представители государственных органов безопасности, администраторы крупнейших фирм. Более того, некоторые из известных хакеров активно участвуют в государственных и международных организациях по информационной безопасности. Так, например, президент и основатель "Chaos Computer Club" (Клуб компьютерного хаоса) Энди Мюллер-Мэган входит в состав всемирной организации ICANN (Internet Corporation for Assigned Names and Numbers). Организованы ха-

керские школы всех уровней для детей (Гражданская школа хакеров), студентов (Foundstone-s hacking school) и сотрудников безопасности (Black Hat Briefings, Ethical Hacking).

В то же время существует опасность взаимодействия хакеров с мафиозными структурами и террористическими организациями. Сформировался и развивается особый вид бизнеса "аренда хакеров". Фирма "Chicago-based 69 Hacking Services" (Служба чикагских хакеров) за умеренную плату (всего от $ 850) предлагает услуги по взлому компьютерных сетей школ, компаний, корпораций и правительств.

Мировоззренческие принципы хакеров активно пропагандируются в средствах массовой информации. Помимо сайтов и порталов, конференций и съездов ценности хакерской субкультуры широко представлены в печатной продукции. Издательства многомиллионными тиражами выпускают литературу, пропагандирующую их деятельность. В России в 2001-2002 гг. вышли сразу три книги Максима Левина: "Библия хакера", "Хакинг с самого начала: методы и секреты", "Методы хакерских атак". Спрос на книгу "Библия хакера" столь велик, что ее коммерческая цена достигла 20800 рублей. Крупнейшие издательства, например "Альянс-Пресс", имеют специализированные серии - в данном случае "Основы хакинга и фрикинга", выпускающие своего рода "учебные пособия" по взлому [14].

В условиях глобальной информатизации, выдвижения на первый план методов информационной войны и промышленного шпионажа изучение субкультуры хакеров приобретает стратегическое значение. В условиях активизации хакерских атак предотвращение разрушительной деятельности хакеров и привлечение их к конструктивной деятельности - важнейшая задача обеспечения национальной безопасности в информационной сфере. По данным "Computer Security Institute" (Института компьютерной безопасности) ущерб от действий хакеров в 2001 г. составил 377,8 млн. долларов против 265,6 млн. долларов в 2000 г. Согласно информации Computer Emergency Response Team (Служба реагирования на компьютерные инциденты), ведущего статистику несанкционированного вторжения с 1988 г., число только зарегистрированных инцидентов в 2003 г. составило 42586, общее же количество преступлений достигло 225049. Фирмы неохотно сообщают о взломах и, как считают эксперты, официальные данные составляют лишь 3% от количества реальных вторжений, которые в ближайшем будущем составят несколько миллионов.

В России также отмечается рост компьютерной преступности. Он сопоставим с темпами компьютеризации страны. Для борьбы с хакерами создано специальное Управление "К" МВД РФ. По данным пресс-службы Управления, сегодня для России характерен рост компьютерной преступности вширь. Взломами занимаются представители самых различных возрастных категорий и социальных слоев населения. В 2002 г. совершено 3,5 тысячи подобных правонарушений, что в 3,5 раза больше, чем в 2001 г.; в 2003 г. только в первом квартале их уже насчитывалось 2850.

К причинам интенсивного роста деятельности хакеров можно отнести: институализацию и ведение целенаправленной пропагандистской деятельности; заинтересованность государственных и криминальных структур в сотрудничестве с хакерами, что способствует резкому повышению их самооценки; привлечение известных хакеров на престижные должности в ведущие фирмы; романтизацию образа хакера средствами массовой информации.

Наряду с изучением общих тенденций развития хакерской субкультуры немаловажен анализ хакерства в рамках той или иной культурно-исторической традиции.

Национальные традиции и хакерство

В субкультуре хакеров наблюдаются специфические особенности поведения этой когорты в зависимости от того или иного типа культуры и менталитета.

Американский тип отличают: мораль индивидуалистического успеха; разрыв с культурным прошлым и интерпретация традиционализма как свидетельство отстало-

сти; идея американской исключительности; установка на выполнение "мировой миссии" гегемона [15], целенаправленное формирование специфических черт американских хакеров. Они гораздо чаще действуют из личных побуждений (например, по соображениям саморекламы), чем русские или европейцы. Большинство американских хакеров - подростки, которые выучили несколько приемов работы с простейшими программами (скриптами) и теперь изменяют главные страницы сайтов "ради тренировки". Такие выводы эксперты делают на основании статистики сайта Attrition.org, где видно, что с 1995 г. атакам подверглись около 3,5 тысяч сайтов в зоне ".com" (коммерция) и только 34 сайта в зоне ".fr" (Франция), 98 в зоне ".de" (Германия) и 22 в зоне ".ie" (Ирландия).

Европейские хакеры более склонны учиться самостоятельно, разрабатывать уникальные методики взлома и обнаружения "дыр" в программном обеспечении. Они воздерживаются от взлома известных сайтов и саморекламы в средствах массовой информации, реже сообщают о своих подвигах в чатах и веб-конференциях, как это делают их американские коллеги. Однако, по мнению американских специалистов, европейцы чаще взламывают сайты в знак протеста против чего-либо или в защиту прав человека.

Азиатский (китайский, сингапурский, японский и т.д.) тип значительно отличается от американского и европейского. Для него характерны: доминирование коллективистского начала; приоритет общественных целей над личными; авторитет власти и иерархии, рассмотрение их как явлений, определяемых естественно-природными, космическими закономерностями; ориентация на семейный характер отношений во всех структурах общества (в корпорации, в государстве); приоритет этических отношений перед стремлением к экономической выгоде (главное - "не потерять лица"); установка на достижение консенсуса (конформизм) [15]. Соответственно складывается и отношение к хакерству. Китайские хакеры более склонны сотрудничать с государственными структурами. Это во многом связано с государственной политикой Китая, уделяющей мерам безопасности особое внимание. Контроль Интернета осуществляется на государственном уровне как с помощью сетевых экранов, так и за счет контроля провайдера за сетевой активностью клиента.

Особое отношение к хакерам возникло в Финляндии в силу специфических социокультурных условий информатизации в этой стране. Обостренное национальное самосознание, обусловленное относительно поздним обретением государственной самостоятельности и стремлением сохранить культурную самобытность в условиях вхождения в Европейский Союз (1995 г.), определили своеобразие финской модели информационного общества [16]. *Финский* тип отличают: доминирование национальной идеи возрождения; приоритетная значимость государственных инициатив; установка на сохранение культурной идентичности, значение социальных программ поддержки населения средствами новых информационных технологий; открытый характер информационного общества (коллективная разработка стандартов, программного обеспечения, инновационных проектов); отсутствие иерархии, причастность к достижениям новых информационных технологий всех слоев общества; положительное отношение к технологиям и информатизации населения, отсутствие движений антиглобализма, низкая общая и компьютерная преступность [15].

Это, в свою очередь, привело к формированию информационной культуры нового типа, в терминах Химанена - "культуры хакеров", совмещающей в себе национальные корни и глобальные тенденции. Отношение к технологиям, как своего рода народному достоянию, позволяющему выжить, породило специфическую ситуацию открытости инноваций. П. Химанен считает, что фактором успешного развития информатизации общества в Финляндии явилась хакерская этика как основа инновационной культуры. В книге "Хакерская этика и дух информационного века" [17] Химанен рассматривает хакеров в первоначальном смысле данного понятия - как новаторов. Главной ценностной установкой ранних американских хакеров и их финских коллег было убеждение в необходимости открытого для всех программирования.

Но американцы достаточно быстро отказались от этого принципа. Американские компании, в частности знаменитая Microsoft, в погоне за прибылью, постоянно модернизируя программы и выпуская на рынок "недоработанную" продукцию, закрыли исходные коды. В отличие от американцев, финны, разрабатывая свой знаменитый Lunex (операционную систему) на общественных началах и выкладывая все исходные коды, объединили усилия с тысячами специалистов в мире. Создатель начального варианта Lunex Линус Торвальдс глубоко убежден, что операционные системы должны быть общим достоянием, как, например, дороги. В Финляндии считают, что открытость является важной стратегической установкой, позволяющей получить конкурентные преимущества не только в борьбе за рынки сбыта, но и в социальном плане. Привлекается опыт не только программистов, но и пользователей. При таком подходе возникает новая этика "обратимости права", подрывающая предпосылки возникновения компьютерной преступности. Интернет создает идеальные условия для реализации этой модели, инновационный потенциал которой в эпоху информационно-технологической революции играет решающую роль. Возможности для коллективного творчества получают качественно новый импульс. Это порождает и новый социальный эффект, направленный на достижение гармонии и взаимопонимания представителей различных наций и культур, возможность существования хакерства только в положительном, инновационно-творческом смысле.

Российский тип хакеров обусловлен общими чертами культурного развития нашей страны: неопределенностью самосознания и поиском культурной идентичности; бинарным характером существования и развития культуры; коллективизмом сознания, отрицающего иерархию; отношением к власти и законам как внешнему, чуждому элементу; установкой на восприятие руководителя государства как защитника народа и противопоставлением его бюрократическим структурам. Характерно и двоякое отношение к хакерам, - с одной стороны, отождествление их с преступниками, с другой - стремление увидеть у начинающих хакеров творческий импульс, требующий государственной и общественной поддержки.

Предприняты первые попытки сформировать обобщенный портрет русского хакера. Согласно данным Экспертно-криминалистического центра МВД России, русский хакер - это подросток или мужчина в возрасте от 15 до 45 лет, как правило, не привлекавшийся к уголовной ответственности; владеющий компьютером в диапазоне от начального до высокопрофессионального уровня; добросовестный работник, но с завышенной самооценкой, нетерпимый к насмешкам, потере социального статуса; отличается ярко выраженной индивидуальностью, обычно скрытен, любит уединенную работу, мало общителен. Русские хакеры в большей степени предрасположены к идеологическому обоснованию взломов, чем их собратья за рубежом. Примером может служить взлом сайта ФБР во время бомбежек Югославии, критика деятельности Microsoft, выпускающей на рынок некачественную с точки зрения информационной безопасности продукцию, взлом сайтов без нанесения ущерба в целях манифестации имеющихся "дыр" в системе безопасности. Можно согласиться с начальником одного из отделов Управления "Р" Д.В. Чепчуговым в том, что "Хакеры - это не преступники, хакеры - это в большинстве талантливые ребята, а преступники те, кто вовлекает их в совершение преступления" [18].

Заключение

Завершая рассмотрение поставленной проблемы, необходимо отметить, что объективные процессы нарастающей мировой глобализации, развитие Интернета, электронной коммерции, активизация террористических организаций создают необходимость концентрации усилий для борьбы за информационную безопасность. На протяжении 2000-2001 г. проведен ряд важных международных совещаний: саммит Большой

восьмерки по вопросам преступности в Интернете (Париж - 2000); конференция стран Большой восьмерки по информационной безопасности (Берлин - 2000).

В 2001 г. 30 стран, включая США, подписали "Конвенцию о киберпреступлениях", устанавливающую общие для стран-участников методы борьбы с нарушителями закона в Сети. Конвенция конкретизирует уголовные и гражданско-правовые санкции за хакерство, нарушение авторских прав и детскую порнографию. Договор содержит также меры предосторожности, введенные в связи с сентябрьскими терактами в США, что дает странам-участникам равные права для контроля информации о подозреваемых в терроризме, передаваемой через Интернет.

Принятие этих актов позволяет, с одной стороны, снизить рост киберпреступности, а с другой, - создает возможность тотального контроля над личностью. В то же время развитие глобализации в борьбе с преступлениями в Интернете не должно идти по пути создания "киберполиции", стоящей выше государственных границ и национального суверенитета, на чем настаивают США. Европейские страны намерены строить свои отношения на принципах международного сотрудничества, охраны частной собственности и личной жизни.

Наряду с общими международными усилиями не менее важны и усилия внутри стран, использующих новые информационные технологии, по активизации воспитательной, разъяснительно-пропагандистской работы. Необходимы также государственные инициативы и меры, направленные на создание условий для активной творческой деятельности молодежи, недопущение вовлечения ее в криминальные структуры.

СПИСОК ЛИТЕРАТУРЫ

1. Приоритетные проблемы научных исследований в области информационной безопасности Российской Федерации / *Стрельцов А.А.* Обеспечение информационной безопасности России. М., 2002.
2. *Милославская Н.Г., Толстой А.И.* Интрасети: доступ в Интернет. Защита. М., 2000.
3. *Осипов Е.* Субкультура хакеров: деконструкция или воля к знанию? http://www.cnews.ru/ security /par 7.
4. *Касперски К.* Техника и философия хакерских атак. М., 2001.
5. *Леви С.* Хакеры - герои компьютерной революции. М., 1984.
6. *Тайли Эд.* Безопасность компьютера. Минск, 1997.
7. *Bruce Sterling.* The hacker crackdown. New Years. Day. 1994.
8. *Медведовский И.Д., Семьянов П.В..Леонов Д.Г.* Атака через Интернет. М., 1997.
9. Кто такой хакер? Сайт "hackAttack" http://determion.narod.ru/hacker.html.
10. Большой хакерско-русский словарь, Хакер.ru № 049
11. *Букин М.С.* Субкультура хакеров. М., 2003.
12. *Барлоу Дж.П.* Zhurnal.ru № 1, 1996. 2 октября.
13. Социальная инженерия. Профессиональное программирование. Последовательный взлом. http://www.i2r.ru/static/450/out_16814.shtml.
14. *Макаров А.С.* Теория и практика хакерских атак. М: Альянс-пресс, 2003.
15. *Скородумова О.Б.* Социокультурные функции Интернета и особенности их реализации в современной России. М., 2003.
16. *Химанен П., Кастельс М.* Информационное общество и государство благосостояния: Финская модель. М., 2002.
17. *Himanen Pekka.* The Hacker Ethic and the Spirit of the Information Age (prologue by Linus Torvalds and epilogue by Manuel Castells). New York: Random House, 2001.
18. *Кононов А.А.* Информационное общество: общество тотального риска или общество управляемой безопасности? / Проблемы управления информационной безопасностью. М., 2002.