С.В. МАСЛЕНЧЕНКО,
КАНДИДАТ КУЛЬТУРОЛОГИИ (МИНСК)

СУБКУЛЬТУРА ХАКЕРОВ

Субкультура хакеров выступает репрезентативной моделью внутрикультурных преобразований, происходящих в современной культуре на пути трансформации от индустриальности к постиндустриальности. Хакеры становятся создателями нового ценностно-нормативного комплекса ориентаций молодежи, а также активными инициаторами значительных изменений информационной индустрии. Показано, что субкультура хакеров представляет собой сложноструктурированное внутрикультурное образование: «белые» хакеры, «черные» хакеры, включая кракеров-вандалов, кракеров-шутников, кракеров-пиратов, кардеров, фишеров, фрикеров, спамеров, которые в своей деятельности используют клаберов и геймеров.

The subculture of hackers appears to be a representative model of the intra-cultural transformations in a modern culture taking place on the way from an industrial to a postindustrial epoch. Hackers are turning to both the creators of a new value-norm complex of orientations of the youth and active initiators of considerable changes of the information industry. The subculture of hackers is viewed as an intra-cultural derivation with a complicated structure: it comprises «white» hackers, «black» hackers, including crackers-vandals, crackers-jokers, crackers-pirates, carders, fishers, freakers, spammers who in the activities use club-kids and gamers.

Вторая половина XX в. стала переломной эпохой в зарождении и развертывании информационного общества. Подобные мегатрендовые процессы всегда сопряжены со значительными трансформациями как материальной составляющей цивилизации, так и ее духовного наполнения. Не осталось в стороне от эпохальных изменений и внутреннее пространство культуры, которое освободилось от потерявших актуальность субкультур, а также породило новые внутрикультурные подсистемы. Репрезентативной моделью происходящих в постиндустриальном обществе изменений выступает субкультура хакеров.

Первые публикации по проблематике субкультуры появились в конце 1960-х гг. в прессе США и Европы, что было связано с ростом студенческих

выступлений в этих регионах. Однако эти материалы носили фрагментарный и поверхностный характер. Более систематизированные и комплексные исследования по этому направлению вышли в свет к середине 1980-х гг. В это же время публикации по данной тематике появились и в СССР. Работы, посвященные субкультуре хакеров – внутрикультурному образованию, выстраивающему свою деятельность вокруг программно-технического переустройства цифрового виртуального пространства – Интернета, актуализировались в западной периодике во второй половине 1990-х гг. и носили констатирующий, описательно-статистический характер.

Анализируя материалы о компьютерном мире, нельзя не обратить внимание на тот факт, что ни в одном из них не проводится грань, четко разделяющая всех, так или иначе связанных с компьютерной безопасностью. Представители первого поколения хакеров утверждают, что они сами дали рождение термину «хакер», построили Интернет, создали операционную систему Unix, управляют Usenet, обеспечивают работу World Wide Web. В рамках данной культурной среды до сих пор действует правило: если человек является частью этой культуры, внес в нее свой вклад и другие члены этой культуры знают о нем и называют его хакером, то он – хакер.

Всех представителей данной субкультуры можно разделить на **хакеров** (hackers) и **кракеров** (crackers). И те и другие во многом занимаются решением одних и тех же задач – поиском уязвимости вычислительных систем. Принципиальное различие между ними состоит лишь в преследуемых целях. Основная задача хакера – исследуя вычислительную систему, обнаружить слабые места в системе ее безопасности и информировать об этом пользователей и разработчиков системы с целью последующего устранения найденных недостатков. Основная же задача кракера – в непосредственном осуществлении взлома системы с целью получения несанкционированного доступа к чужой информации, иначе говоря, для ее кражи, подмены или объявления факта взлома.

Анализ изменений в сфере технического обеспечения коммуникации во второй половине XX в. позволяет говорить о нескольких «поколениях» хакеров, которые способствовали становлению данной субкультуры и информационно-технологическому прогрессу в силу своей деятельности:

– первое поколение хакеров на начальном этапе занималось созданием и преобразованием огромных по размерам первых компьютеров с использованием так называемой технологии доступа разделения времени;

– вкладом второго поколения явилось изобретение в конце 1970-х гг. персональных компьютеров;

– третье поколение хакеров в начале 1980-х гг. разработало большое количество прикладных программ для персональных компьютеров, которые способствовали успеху платформы IBM. Созданные ими организации, такие как «Фонд электронных рубежей» (Electronic Frontier Foundation), и в настоящее время серьезно влияют на политику Вашингтона в области соблюдения гражданских прав в киберпространстве;

– четвертое поколение создало то, что принято теперь называть киберпространством, или Интернетом, – средой обитания и общения нескольких сотен миллионов человек. Возникает еще одно гениальное изобретение, интегрированное в эту среду, – система сенсорного погружения, или так называемая виртуальная реальность, начальные основополагающие принципы и концепция которой были разработаны одной из ярких личностей первого поколения хакеров – Дж. Ланье. На более ранних стадиях труд представителей четвертого поколения хакеров можно было видеть в объективации систем электронной почты на основе BBS (Bulletin Board System) – электронной доски объявлений, а также сети USENET, созданной в начале 1980-х гг. (от USER'S NETWORK – сеть пользователей) Т. Траскоттом и Д.-Дж. Эллисоном. Здесь впоследствии очень точно был сформулирован

важный принцип всех поколений хакеров – «участвовать может любой». Да и сама USENET может считаться эталоном в плане своей структуры – полная децентрализация, отсутствие иерархии, самоорганизация и резкое отрицание любого коммерческого использования. Именно четвертое поколение хакеров активно противостоит коммерциализации и узурпации какими-либо государственными органами региональных и опорных высокоскоростных коммуникационных магистралей Интернета, руководствуясь правом всеобщей доступности и бесплатности информации.

Сейчас представители субкультуры хакеров – это виртуальное сообщество, располагающее в сети значительными информационными и интеллектуальными ресурсами и механизмами самоорганизации своей деятельности. Известно несколько тысяч хакерских сайтов, издаются многочисленные электронные журналы для хакеров, среди них наиболее известные «CRASH», «40Hex», «2600», «TAP», «Hackers Unlimited», «Жаргон», «Хакер». В актуальном состоянии поддерживаются каталоги хакерского софта, в том числе постоянно обновляемого хакерского инструментария по снятию защиты с игр, а также снятию защиты от копирования, взлома, сканирования и расшифровки паролей, маскировки данных в звуковых и графических файлах, сканирования адресов IP, создания вирусов.

За несколько десятилетий своего существования субкультура хакеров объективировала многочисленные ценностные ориентиры и модели поведения. Однако ценности хакеров не представляют собой строгую однозначную и всеми принимаемую систему. Общее, что нашло объективацию в большинстве сегментов данной субкультуры, – свобода информации, доступа к ресурсам и распространения программного обеспечения.

Наиболее известные хакерские ценностные системы были предложены представителями первого поколения, базирующегося на технической культуре MIT, – С. Леви, Л. Блэнкеншипом, Э.-С. Рэймондом, А. Ламо.

В 1984 г. С. Леви в своей знаменитой книге «Хакеры: Герои компьютерной революции» сформулировал принципы «хакерской этики»:

«Доступ к компьютерам должен быть неограниченным и полным».

«Вся информация должна быть бесплатной».

«Не верь властям – борись за децентрализацию».

«Ты можешь творить на компьютере искусство и красоту».

«Компьютеры могут изменить твою жизнь к лучшему»[1].

Сокращенной моделью системы ценностных ориентиров хакеров выступает «Манифест хакера», написанный 8 января 1986 г. Л. Блэнкеншипом, более известным как Наставник (The Mentor). Автор называет основные ценности культуры хакера: безразличие к цвету кожи, национальности и религии, превосходство знаний и нестандартного образа мыслей, безграничная свобода информации для исследования, изучение из любопытства. В 1995 г. отрывок из «Манифеста» был зачитан в фильме «Хакеры», а также его текст воспроизведен в компьютерной игре Uplink.

Наиболее развернутая модель, позволяющая реконструировать духовный мир хакеров, представлена хакером первого поколения Э. Рэймондом, одним из родоначальников экспериментов с ARPANET, соавтором программного обеспечения Unix, редактором веб-журнала «Жаргон»: писать программы, доступные для всех, помогать тестировать и отлаживать такие программы, публиковать полезную информацию, помогать поддерживать работу инфраструктуры Интернета, служить самой хакерской субкультуре. Пути формирования навыков хакера: изучать методы программирования на основании языков Python, Си, Perl и LISP посредством чтения и написания кодов, научиться использовать один из вариантов Unix в исходных кодах и работать с ним, применять World Wide Web и писать на HTML, что позволит лучше понимать и изменять Интернет. Статус в хакерской субкультуре

строится на репутации. Субъектами оценки выступают только равные (в техническом и программном смысле) соискателю или превосходящие его.

В зависимости от мотивов деятельности субкультура хакеров делится на следующие группы:

1. **«Белые» хакеры** – малочисленная группа киберпользователей, ставящая целью своей правомерной деятельности оказание помощи программистам и пользователям в совершенствовании управления компьютером и виртуальными сетями, модернизации и создании новых программ, в борьбе с «черными» хакерами – кракерами. Оценка просоциальности данной группы хакеров в большей степени зависит от толкования правом их деятельности, а не от мнения большинства пользователей, которые, как правило, высказывают одобрение действиям кракеров, дающих возможность киберсообществу нелицензионно, бесплатно, неограниченно пользоваться продуктами программного обеспечения и компьютерными сетями независимо от решения правообладателя.

Значительная часть «белых» хакеров – бывшие кракеры. Многим получить статус «белого» и избавиться от преследования, а в некоторых случаях и приобрести известность помогает деятельность на благо общества под пристальным вниманием правоохранительных органов и высокотехнологичных компаний.

В большинстве случаев жизнь «белых» хакеров носит публичный характер. Крупные компании выступают инициаторами и финансовыми организаторами проведения различных международных off- и online-конференций, чемпионатов в сфере высоких технологий, преследуя, как правило, экономические цели: заметить и завербовать на работу подающего надежды молодого специалиста. В последние годы наибольшей известностью и престижем пользуются чемпионат Google по программированию и чемпионат мира по программированию среди студентов (International Collegiate Programming Contest).

2. **«Черные» хакеры, или кракеры,** – самая опасная группа в среде киберпользователей, занимающаяся несанкционированным доступом к сетям и информации, что приносит существенный ущерб определенному количеству пользователей. Результатом их работы являются «кряки» и генераторы ключей (в случае ориентации на массового пользователя) или же просто модифицированная (взломанная) программа с нужной функциональностью. В подавляющем большинстве стран деятельность по взлому программ считается противозаконной (в том числе в России и Беларуси, однако статус «кряков» и кейгенов как вредоносного ПО пока не определен).

«Кракерская» атака – действие, целью которого является захват контроля (повышение прав) над удаленной/локальной вычислительной системой, либо ее дестабилизация, либо отказ в обслуживании.

Можно выделить следующие наиболее распространенные методы «кракерской» атаки:

Mailbombing – самый старый метод атак: рассылка большого количества почтовых сообщений, которые делают невозможными работу с почтовыми ящиками, а иногда и с целыми почтовыми серверами.

Подбор пароля – вид атаки, при которой взломщик подбирает пароли к системам ограничения доступа.

Вирусы, троянские кони, почтовые черви, снифферы, Rootkit-ы и другие специальные программы – это использование специальных программ для ведения работы на компьютере жертвы. Такие программы предназначены для поиска и передачи своему владельцу секретной информации либо нанесения вреда системе безопасности и работоспособности компьютера жертвы.

Сетевая разведка – получение «кракером» закрытой информации о построении и принципах функционирования вычислительной системы жертвы.

Сниффинг пакетов – распространенный вид атаки, основанный на работе сетевой карты в режиме promiscuous mode. В таком режиме все пакеты, полученные сетевой картой, пересылаются на обработку специальному приложению. В результате злоумышленник может получить большое количество служебной информации: кто, откуда, куда передавал пакеты, через какие адреса эти пакеты проходили. Самой большой опасностью такой атаки является получение самой информации, например логинов и паролей сотрудников, которые можно использовать для незаконного проникновения в систему под видом обычного сотрудника компании.

IP-спуфинг – распространенный вид атаки в недостаточно защищенных сетях, когда злоумышленник выдает себя за санкционированного пользователя, находясь в самой организации или за ее пределами.

Man-in-the-Middle – вид атаки, когда злоумышленник перехватывает канал связи между двумя системами и получает доступ ко всей передаваемой информации.

Инъекция – внесение некоторых сторонних команд или данных в работающую систему с целью получения доступа к закрытым функциям и информации либо дестабилизации работы системы в целом.

SQL-инъекция – атака, в ходе которой изменяются параметры SQL-запросов к базе данных. В результате запрос приобретает совершенно иной смысл и способен не только произвести вывод конфиденциальной информации, но и изменить/удалить данные.

PHP-инъекция – способ взлома веб-сайтов, работающих на PHP, заключающийся в выполнении нужного кода на серверной стороне сайта.

Межсайтовый скриптинг, или **XSS** (от англ. Cross Site Scripting) – атака, аналогичная SQL-инъекции, но для проведения этой атаки кракер меняет не SQL-запрос, а внутренние переменные действующей системы (например, переменные окружения PHP, Perl и т. д.), используя недочеты в обработке входных параметров скриптов либо ошибки в настройке скрипт-обрабатывающих приложений.

Социальная инженерия (от англ. Social Engineering) – использование некомпетентности, непрофессионализма или небрежности персонала для получения доступа к информации. В ходе такой атаки кракер устанавливает контакт с жертвой и, вводя ее в заблуждение либо войдя в доверие, пытается получить необходимые сведения, которые сложно получить другим путем, а другие пути являются более рискованными.

Отказ в обслуживании DOS (от англ. Denial of Service) – атака, цель которой – доведение системы жертвы до отказа.

DDOS (от англ. Distributed Denial of Service – распределенная DOS) – подтип DOS-атаки, имеющий ту же цель, но производимый не с одного компьютера, а с нескольких компьютеров в сети; используется там, где обычный DOS неэффективен. Для этого несколько компьютеров объединяются, и каждый производит DOS-атаку на систему жертвы.

Основным инструментом деятельности как у «черных», так и у «белых» хакеров выступает вирус – специально созданный программный код, способный самостоятельно распространяться в компьютерной среде.

В последнее время активность «черных» хакеров растет огромными темпами, о чем свидетельствует активизация деятельности антивирусных компаний. Так, лидер антивирусного рынка России Лаборатория Касперского в ноябре 2004 г. перешла на ежечасное обновление баз данных. До этого пользователи имели возможность загрузки свежих обновлений через каждые три часа; для примера: в 2000 г. базы обновлялись 63 раза, 2001 г. – 205, 2002 г. – 652, 2003 г. – 818, а за первые семь месяцев 2004 г. – свыше 1500 раз[2].

Между вирусописателями развернулись настоящие соревнования на быстроту и масштабы заражения ПК, а также инновационность в разработке

вредоносных кодов. Так, в 2006 г. появилось 60 тыс. новых вирусов, в 2007 г. только Лабораторией Касперского было обнаружено 220 172, а в 2008 г. – 189 785 новых вредоносных программ. Экономический ущерб от вирусов в 2001 г. составил примерно 13 млрд, в 2002 г. – 20–30 млрд, в 2003 г. – 55 млрд USD, основной источник заражения – спам[3], в 2004 г. – 166–202 млрд USD (по данным NG.ru). По подсчетам Cnews.ru, общий ущерб, нанесенный мировой экономике кракерами составил в 2002 г. 125, в 2003 г. – 215, в 2004 г. – 411, а с 2005 г. – более 500 млрд USD ежегодно.

С 2007 г. в среде кракеров наметились следующие тенденции: стремительный рост числа троянских программ-шпионов, ориентированных на кражу данных пользователей online-игр; активное использование хакерами систем мгновенного обмена; стремительная экспансия вредоносных программ в те области интернет-деятельности, которые ранее оставались относительно безопасными, – online-игры и социальные сети; применение все новых способов противодействия антивирусным компаниям – упаковки, шифрования, замусоривания вирусного кода.

Разные исследователи по-разному оценивают перспективы борьбы с вирусной опасностью, однако преобладают пессимистические прогнозы. С большой долей вероятности можно утверждать, что борьба с компьютерными вирусами будет крайне долгой и, вероятно, безуспешной.

Однако было бы несправедливым полагать, что кракеры представляют собой органическое единство. Их можно разделить на несколько групп в зависимости от цели, с которой осуществляется взлом.

Вандалы – самая известная (во многом благодаря широкому распространению вирусов, а также публикациям некоторых журналистов) и самая малочисленная часть кракеров. Их основная цель – взломать систему для ее дальнейшего разрушения.

Шутники – наиболее безобидная часть кракеров, которые стремятся к известности путем взлома компьютерных систем и внесения туда различных эффектов, выражающих их неудовлетворенное чувство юмора.

Взломщики – профессионалы, пользующиеся наибольшим почетом и уважением в кракерской среде. Их основная задача – взлом компьютерной системы с целью кражи, подмены или уничтожения хранящейся там информации.

Пираты – кракеры, ворующие свежие (warez на жаргоне) программы с помощью средств, самостоятельно разработанных или заимствованных у других лиц. Внутри группы кракеров-пиратов можно выделить определенную специализацию: **пираты-взломщики** (взлом компьютерной защиты), **пираты-курьеры** (копирование ворованного программного обеспечения на свой компьютер), **пираты-дистрибьюторы** (занимаются распространением ворованного ПО). Корыстная мотивация людей, входящих в пиратские группы, вполне очевидна. Но речь не обязательно идет о деньгах – в качестве платы за свежие программы принимается либо другой warez, либо адреса компьютеров со взломанной защитой. Поскольку дыры в компьютерной защите выявляются, «штопаются» довольно быстро (как правило, от нескольких часов до недели), адреса взломанных систем пользуются огромным спросом.

Шпионы – кракеры, охотящиеся за секретной информацией. Обычно они работают на заказ и за большое вознаграждение на военных, разведку и т. д. Конечно, вторжение в компьютеры, отвечающие за национальную безопасность, – любимое развлечение «экспериментаторов», однако, как считают эксперты, за внешне невинными и хаотическими «экспериментами» могут скрываться и организованные разведывательные акции. В последнее время эта модель активности приобретает новую форму – «боевой езды» (war driving – на языке кракеров): кракеры-«шпионы» разъезжают по городу

в поисках незащищенных Wi-Fi-сетей. При обнаружении таковых по беспроводному каналу они внедряют в атакуемую компьютерную сеть spyware-программу, с помощью которой перехватывают информацию. Как правило, это данные о реквизитах кредитных карт клиентов. Затем кракеры действовали по известной схеме: взлом банковской сети или сети магазинов, которыми пользовался владелец карты, и перевод денег на свои офшорные счета.

Кардеры (от англ. *carding*) – кракеры, использующие чужие (ворованные) кредитные карты для электронной оплаты товаров или услуг. Наиболее распространенным методом воровства номеров кредитных карт на сегодня выступает фишинг. Частным случаем кардинга является скиминг, при котором используется скимер – инструмент злоумышленника для считывания, например, магнитной дорожки кредитной карты; представляет собой миниатюрное устройство со считывающей магнитной головкой, усилителем-преобразователем, памятью и переходником для подключения к компьютеру.

Фишеры – интернет-мошенники, выдающие свои страницы за сайты других. Обычно они маскируют ссылки на свои сайты, копируют дизайн популярных ресурсов и требуют на специально созданных веб-страницах ввести пароль пользователя или данные о его кредитной карте.

Фрикеры – субъекты, осуществляющие взлом телефонных автоматов и сетей обычно с целью получения бесплатных звонков или связи с Интернетом.

Спамеры – самое многочисленное и структурно-пестрое внутригрупповое образование в кракерской среде, занимающееся формированием и рассылкой спама – непрошеной корреспонденции рекламного характера.

В спамерской среде можно выделить следующие группы:

1. **Спамеры-кракеры** создают программы: для сбора адресов с сайтов и форумов (сетевые пауки), быстрой массовой рассылки, проверки существования и работоспособности адресов, захвата компьютеров пользователей и превращения их в машины для рассылки спама. По данным Лаборатории Касперского, каждый день в мире появляется не менее 20–30 тыс. новых IP-адресов, рассылающих спам (преимущественно зараженных машин), причем только примерно 10 тыс. из них попадают в публичные черные списки.

2. **Спамеры-собиратели баз данных** обслуживают нужды рассыльщиков и собирают для них почтовые адреса, которые объединяют в базы адресов. Они используют программное обеспечение, созданное спамерами-кракерами и обладающее возможностью собирать адреса в Интернете, проверять их работоспособность, помещать в базу. Тут применяются разнообразные методы – от кражи адресов у провайдера (через завербованных агентов) до подбора адресов «на кончике пера» (с помощью различных эвристических алгоритмов и так называемых словарных атак).

3. **Спамеры службы рассылок** – это, собственно, и есть чистые спамеры – те, кто рассылает спам; как правило, представлены десятками крупных спамерских фирм, сотнями мелких фирм и отдельных профессионалов, тысячами непрофессионалов (студентов, безработных).

По данным исследований, 64–83 % электронной почты в мире – спам[4]. Исследования компании Sophos в 2006 г. показали, что из США рассылается больше спама, чем из остальных регионов, вместе взятых. В процентном отношении показатели выглядят следующим образом: США – 56 % мирового спама, Канада – 6,8 %, на третьем месте – Китай и Гонконг, на четвертом – Южная Корея. На начало 2007 г., согласно исследованию компании Marshal, доля спама составляла примерно 85 % общего количества корреспонденции.

Для совершения спамерских и вообще вирусных атак кракеры в последние годы проявляют все большую склонность к объединению в группы. Посредством Интернета устанавливаются связи между разрозненными представителями как внутри определенной страны, так и за ее пределами. Такие

группы известны определенными связями со спам-сообществом, охотно приобретающим у них сети из зараженных троянскими программами компьютеров, и опираются на «сервисную» индустрию, представляющую собой миллионы «неполноценных» или потенциальных кракеров как слепое орудие противоправных действий против систем защиты частной и корпоративной информации. Размер нового рынка уже составляет 1,5–3 млрд USD в год.

В результате корпоративным и личным системам безопасности предстоит столкнуться с угрозами совершенно нового рода – потенциально миллионной армией киберпреступников, опирающихся на поддержку «сервисных» кракеров. В качестве социальной базы индустрии, обслуживающей кракеров, традиционно выступают **клаберы** (от слова клуб) **и геймеры** (от слова игра), две категории киберпользователей, которые тесным образом связаны между собой и обладают достаточными навыками работы с компьютером, а также с локальными сетями и Интернетом. Зная их стремление к игре в рамках сетей, кракеры используют геймеров как агентов, разносящих вирусосодержащее программное обеспечение и спам.

Современная субкультура хакеров немыслима без Интернета. Администрирование всемирной сети, поддержание универсальной свободной безопасной коммуникации – основная задача «белых» хакеров. В российском и белорусском сегментах Интернета приблизительно до 2000 г. функцию системных администраторов выполняли только хакеры-самоучки. По мере расширения государственного участия в цифровом информационном пространстве администрирование в сети начало осуществляться специалистами, подготовленными в высших учебных заведениях. С этого момента «белые» хакеры совместно с системными администраторами, которые не обязательно поддерживают ценности хакеров, противостоят кракерским атакам, обеспечивают стабильность и поступательный рост темпов и масштабов дальнейшего развития сети, придавая ей все больше черт социальной реальности и обеспечивая актуализацию:

– **политической интернет-сферы,** которая позволяет гражданам осуществлять свои политические и гражданские права и обязанности через систему формальных и неформальных виртуально представленных общественных организаций и политических институтов, включая электронное правительство – новую модель государственного управления, построенную на возможностях современных информационных технологий;

– **сферы интернет-коммерции,** набирающей значительные экономические темпы и масштабы охвата аудитории, достигнув в 2007 г. объема в 400 млрд USD, создающей свое собственное производство, которое обеспечивает создание дополнительных рабочих мест – веб-порталов и сайтов;

– **правовой интернет-сферы**, центральным ядром которой выступают проблемы государственного и межгосударственного регулирования этой сферы жизнедеятельности, противодействия кракерской преступности, которое выражается в разработке электронного законодательства, в первую очередь защищающего военные, экономические и политические интересы отдельных государств и международных организаций. ООН предпринимает шаги по укреплению нейтралитета, ответственности и всеобщего характера Интернета и продолжает устранять препятствия на пути интернационализации способов принятия решений;

– **духовной сферы**, которая характеризуется существенным участием религиозных, научных и художественных институтов в глобальной сети. И если наука заявляет о себе, как правило, через размещение информации описательного познавательно-просветительного характера, то религиозные учреждения, организации, реализующие себя в искусстве, как, собственно, сами деятели искусств, пытаются перенести свою деятельность в киберпространство.

Современный Интернет приобретает все больше черт социальной реальности. В нем зарождаются и функционируют виртуальные социальные институты и группы, осуществляется реальная экономическая деятельность, создаются собственное производство и сфера услуг, объективируются новые отрасли экономики и трудовой активности населения, значительно расширяется сфера отдыха, реализуются новые аспекты индустрии развлечений, все больший удельный вес набирают религиозная и художественная сферы. Эти процессы происходят на фоне постоянного роста интернет-населения и расширения его географического влияния, что вызывает объективную необходимость не только в осуществлении общего регулирования и поддержания порядка, но и в защите прав и интересов пользователей, поскольку всемирная сеть становится сферой взаимодействия не только законопослушных граждан, но и преступников. А пока правительства пытаются разработать формально-правовые регуляторы Интернета, хакеры самостоятельно, в большинстве случаев на неформальном уровне обеспечивают свободное функционирование.

Таким образом, современному гуманитарному знанию предоставляется редкая возможность понять динамику и последствия стратификационных и ролевых изменений в постиндустриальном обществе при исследовании субкультуры хакеров, генезис и трансформация которой происходили в результате смены ряда технических культур, создавших условия для трансформации компьютерных стратегий и разработки новых технологий записи, хранения, передачи и использования информации.

[1] Масленченко С.В. Субкультура и коммуникация. Мн., 2003. С. 66.

[2] См.: Саевич Д. Еще более активный ответ новым вредным угрозам // Компьютер. газ. 2004. 16 авг. С. 29.

[3] См.: Платов А. Кое-что о вирусах // Там же. 26 янв. С. 5.

[4] См.: Кононович А. ФБР начинает войну со спамерами // Компьютер. вести. 2004. 27 мая. С. 3.

Поступила в редакцию 25.06.09.