Т.Е. Савицкая

Современный компьютерный андеграунд: крах мечты?

Ил. 1.

Как известно, одна из составляющих сложного генезиса современной глобальной электронной цивилизации – западная контркультура 60–70-х годов прошлого века. Точнее – это выросшие в недрах либертарианского мейнстрима виртуальные сообщества киберхиппи, а позднее киберпанков, в борьбе с истеблишментом за право на свободное самовыражение и коммунитарный эксперимент сформировавших субкультуры фрикеров и хакеров, которые – в свою очередь – внесли существенный вклад в изобретение персонального компьютера, видеоигр, электронной почты, базиса последующей киберкультуры. История формирования компьютерного андеграунда в США и странах Западной Европы на протяжении 60–80-х годов прошлого века в бурную эпоху BBS {Bulletin Board System), «электронных досок объявлений», хакерских войн и первых стычек с полицией была уже предметом нашего рассмотрения.[1]

В последующие десятилетия в период активной интернетизации социума, когда Сеть стала зоной социально-культурного креатива, ареалом новых вполне легальных культурных практик (онлайновые игры, социальные сети, сетевые дневники и проч.), борьба за право на электронное самовыражение для индивидов и групп, вокруг которого формировался прежний компьютерный андеграунд, во многом потеряла смысл. Корпоративный бизнес в сфере высоких технологий ныне не только не игнорирует права индивидуального пользователя, но чутко отслеживает малейшие веяния интернет-моды, неуклонно повышая уровень комфортности пользования новейшими онлайновыми сервисами, а также постоянно расширяя репертуар интернет-услуг.

Кроме того, последовательное обустройство Сети, ставшей средой обитания для миллионов пользователей по всему миру, к началу текущего столетия превратило ее в средоточие активной финансовой, административной, торговой, политической и научной деятельности; кладезь весьма конфиденциальной (а потому дорогостоящей) личной и корпоративной информации. Все это не могло не сказаться на радикальной

[1] См.: *Савицкая Т.Е.* Из истории компьютерного андеграунда: эпоха BBS и Фидонета. Часть 1 // Культура в современном мире. – 2010, № 4. – [Электронный ресурс]. – Режим доступа: http://infoculture.rsl.ru

трансформации как самого понятия компьютерного андеграунда, так и тех задач, которые ставят перед собой его участники.

Особый случай: компьютерное подполье РФ и стран СНГ

Известно, что в силу ряда социально-исторических обстоятельств РФ со значительным опозданием включилась во всемирный информационно-коммуникативный процесс. Однако, двигаясь по модели «догоняющей модернизации», на протяжении двух последних десятилетий Россия активно преодолевает «цифровое неравенство», выходя по ряду социально-демографических параметров новейших интернет-услуг на среднеевропейский и даже мировой уровень.

По данным Мининформсвязи РФ, к началу текущего столетия количество персональных компьютеров в стране каждый год увеличивалось на 16–20%, к 2005 году около 93% государственных организаций имели собственные сайты, треть из них оказывала интерактивные услуги (например, онлайновые консультации) [1]. По уровню популярности социальных сетей (учитывалось среднемесячное количество посещаемых веб-сайтов и затраченное на это время) в 2009 году, как свидетельствует компания ComScore, РФ заняла первое место [2]. По данным Internet World Stats, число пользователей Сети в РФ, в 2000 году составлявшее всего 3 млн. 100 тыс. человек (т. е. примерно 2% населения), в 2010 году насчитывало уже 59 млн. 700 тыс., что составляло 42,8% населения (при среднемировом показателе в 28,7%). Таким образом, по количеству пользователей Интернета РФ вышла на второе место в Европе (после Германии), обогнав Соединенное Королевство (третье место), Францию (четвертое место) и т.д., и на 7-е в мире [3].

Несмотря на успешное, в целом, последовательное преодоление «информационной бедности», рост числа персональных компьютеров, увеличение плотности и скоростных параметров информационных сетей, все большее распространение «цифровой грамотности», ряд социально-экономических факторов неблагоприятно воздействует на процесс информатизации. В первую очередь это неравномерное и недостаточное (особенно в сельской местности и удаленных регионах) развитие социотехнической инфраструктуры, малый имущественный доход; слабое развитие системы скидок и льгот, способных минимизировать весомость для некоторых категорий населения суммы оплаты интернет-услуг. Данные факторы, безусловно, служат стимулом для воспроизводства компьютерного андеграунда, сформировавшегося еще в 90-е годы на волне всеобъемлющего социального коллапса, последовавшего за распадом СССР.

Летом 2004 года в Интернете было опубликовано интересное «Исследование компьютерного андеграунда на постсоветском пространстве», проведенное методом

анкетирования на ряде популярных среди молодежи веб-ресурсов (Bugtrag.ru, Rupor.net, Madalf.ru, Antichat.ru, Frikzona.org и проч.). В процессе анализа было выявлено, что число активных членов организованного компьютерного андеграунда составляет примерно 2 500 человек, из которых в выборочную совокупность попало 103 человека.

В материалах исследования компьютерный андеграунд определятся как «обширная совокупность социокультурных групп, которые различаются по способу самовыражения и самоидентификации в виртуальном пространстве, но при этом едины в своем негативно-позитивном отношении к существующему мировому порядку, с некоторыми небольшими различиями между ними. Люди, которые идентифицируются как агенты «компьютерного андеграунда», стремятся изменить окружающий мир или свое положение в нем посредством информационных технологий «в корыстных или бескорыстных целях» [4].

Ил. 2.

Значительный интерес представляет приведенная в исследовании классификация различных групп компьютерного подполья. Итак, в состав компьютерного андеграунда входят:

1. ***Хакеры-взломщики***, специализирующиеся на «чистых» взломах информационных систем без их повреждения, а зачастую даже с оповещением лиц, ответственных за безопасность данной системы, об обнаруженных в ней недочетах; движущий стимул их деятельности – любопытство исследователя и жажда самовыражения в соответствии с лозунгом «Информация должна быть свободной» (громкий пример такого «чистого» хакерства – взлом осенью 1987 года членами немецкого хакерского клуба «Хаос» крупной научной сети SPAN (Space Physics Analysis Network) американской компании NASA. Полностью захватив контроль над системой, получив доступ к наиболее секретным файлам и проектам, взломщики предупредили руководство NASA об обнаруженных изъянах в безопасности системы и помогли их устранить, в связи с чем были освобождены от судебного преследования);

2. ***Хакеры-вандалы***, планирующие и осуществляющие проникновение в информационные системы с сознательной целью причинения им ущерба, руководствуясь зачастую теми или иными идейными мотивами (протестом против корпоративной политики отдельных компаний, каких-либо социально-политических событий и т.д.);

3. ***Крэкеры или «темные хакеры»***, целенаправленно занимающиеся коммерческим взломом информационных систем, как правило, в интересах наживы;

4. ***Некоммерческие крэкеры-пираты***, осуществляющие взлом закрытых информационных систем с последующим выкладыванием полученных данных в открытом доступе в соответствии с характерной для этой группы трактовкой права пользователя на любую информацию;

5. ***Пираты, специализирующиеся на коммерческих взломах информационных систем с последующей перепродажей полученной информации***; часто группа профессионалов с четко распределенными функциями, работающая по «заданию»;

6. ***Кибер-террористы*** – тесно связанные с криминальным подпольем группы, по идеологическим соображениям нацеленные на нанесение максимального вреда противнику, будь то государство или какая-то группа лиц;

7. ***Санитары*** – небольшая часть андеграунда, в основном сосредоточенная вокруг ресурса cyberarmy.com, ставящая целью очистку Интернета от сетевого вандализма, детской порнографии и проч.;

8. ***Вирмейкеры*** (от англ. «virus» – вирус, и «to make» – делать, создавать), специализирующиеся на написании компьютерных вирусов; другое название – вексеры (от англ. «virus exchange» – обмен вирусами), а также технокрысы. По данным исследователя компьютерного подполья, в этой группе можно вычленить более мелкие подразделения: трейдеров, коллекционирующих компьютерные вирусы из любопытства или с целью обмена; деструкторов, создателей вредоносных вирусных программ; исследователей, изучающих, а иной раз и пишущих вредоносные программы, но не пускающих их в оборот; кодеров, начинающих программистов, «тестирующих» свои силы в написании нестандартного кода, и т.д.

9. ***Кардеры*** (от англ. «card» – кредитная карта) – одна из наиболее закрытых общностей внутри компьютерного андеграунда в силу особого характера своей противозаконной деятельности, практикующая махинации с кредитными картами и взлом банкоматов;

10. ***Фрикеры***, практикующие незаконное подключение к телефонным сетям (некогда основным каналам подключения к компьютерным сетям); по мере развития инфраструктуры Интернета превратившие в объект незаконного проникновения также спутниковую и сотовую связь;

11. ***Прочие «альтернативщики»*** – одиночки или малочисленные группы пользователей, применяющие малораспространенные, нестандартные операционные схемы в качестве способа самовыражения [4].

Каковы же были, согласно предложенному исследованию, социально-демографический состав, ценностные предпочтения и культурные интересы компьютерного андеграунда на постсоветском пространстве начала XXI века?

С помощью анкетирования удалось выявить, что основной возраст его активных представителей – до 25 лет (в том числе значительная прослойка подростков от 14 до 18 лет). Большинство оценивало свое материальное положение как «средний уровень». Преобладающее количество членов компьютерного андеграунда профессионально связано с информационными технологиями не менее пяти лет.

В иерархии потребностей этой группы 1–2 место занимала необходимость самовыражения, опережающая потребности в признании и уважении, безопасности и физическом комфорте. Преобладающее большинство деятелей компьютерного андеграунда считало основными идеями, цементирующими их социокультурную общность, «свободу, независимость», а также «знания, тягу к знаниям», а вовсе не «хаос, анархию» и «стремление заработать». Смысл своей деятельности участники субкультуры в большинстве своем видели в «обеспечении свободного доступа к закрытым информационным массивам», а также в «обеспечении личной приватности» и «сопротивлении корпоративной глобализации». Вполне предсказуемо тяготение опрошенных к поэтизирующим их деятельность фильмам («Хакеры» Й. Софтли, «Матрица» братьев Вачовски), к научной фантастике, книгам киберпанковского направления (Б. Стерлинг, У. Гибсон), хакерским манифестам и киберфольклору.

В какой мере показательны эти данные? Нам представляется, что проведенное исследование в значительно степени адекватно отразило ту стадию развития компьютерного подполья, на которой с достаточным основанием его можно было трактовать как специфическую субкультуру, с одной стороны, акклиматизировавшую на отечественной почве, – со значительным, конечно, опозданием, – ценностно-стилевые и идейные характеристики западной киберкультуры, а, с другой, – подготовившую почву для массовых практик сетевой репрезентации. В связи с этим особую значимость приобретают два фактора, выявленные в исследовании: молодежный по преимуществу состав постсоветского киберподполья (достаточно напомнить, что около 40% анкетируемых – не старше 18 лет) и идейная мотивация их деятельности (обеспечение свободного доступа к информации, тяга к самоосуществлению и новым знаниям).

Бескомпромиссное следование лозунгу «Свобода информации!» приводило к отрицанию права собственности на продукт информационного поиска, переходившего как бы в совместное общинное пользование. Отсюда – свободный обмен файлами в пределах компьютерной субкультуры, выкладывание в открытый доступ «взломанных» программных кодов, всевозможных наработок в сфере нелегальных технических уловок. Молодым людям было лестно считать себя свободными хакерами, пользоваться компьютерным сленгом, следовать заповедям хакерской этики и т.д.

Вскоре, однако, ситуация начала меняться: стремительная экспансия на постсоветское пространство глобальной электронной цивилизации удобств и услуг быстро трансформировала архаичные контркультурные установки компьютерных фанатов в пафос освоения новейших социокультурных практик, предлагаемых формирующимся обществом web 2.0. Массовый пользователь хлынул в социальные сети, электронные дневники (напомним, что по числу пользователей ЖЖ уже в 2007 году РФ вышла на второе, после США, место в мире, которое продолжает удерживать и сейчас [5]); начал осваивать микроблогинг (Твиттер, Twihoo, Трубит.ру и проч.) и мобильный веб. Постсоветское компьютерное подполье вступило в фазу решительных перемен.

Компьютерный андеграунд в РФ: новейшие тенденции

С начала XXI века киберпространство РФ, полноправного члена глобального информационно-коммуникативного процесса, – арена действия общемировых тенденций к большей специализации и профессионализации интернет-услуг, расширению их репертуара и последовательной монетизации. Одно из следствий все большего сращения киберпространства с реальной жизнью во всех ее экономических, социальных, культурно-рекреационных проявлениях – прогрессирующая криминализация киберподполья. По меткому выражению Евгения Касперского, генерального директора одноименной «Лаборатории», «компьютерный андеграунд быстро взрослеет и переходит из разряда «любителей» в лигу «профессионалов» <…>. Время одиночек-альтруистов прошло. Криминальная индустрия и индустрия безопасности оказались лицом друг к другу. Именно этот факт по-настоящему характеризует глубину проникновения и роль информационных технологий в жизни общества» [6].

Легкость распространения преступности в Интернете – оборотная сторона его либертарианской, поощряющей свободу индивида структуры: «паутина ризомы-Интернета не поддается системной и директивной регламентации, … ризоморфное, т.е. номадическое, децентрированное, многомерное, устойчивое к разрывам устройство Интернета» [7] коррелирует с фрагментарностью постмодернистской культуры, поощряющей эгоцентризм и анонимность (по желанию) самопрезентации сетевого индивида. Разумеется, Сети, одному из величайших изобретений человечества за всю историю его развития, не в большей степени может быть инкриминирована недобросовестность отдельных его пользователей, чем изобретателям автомобиля или стрелкового оружия преступное их применение. Бремя свободы, как известно еще с библейских времен, – одно из самых «неудобоносимых».

Резкое сокращение случаев «идейного» хакерства в Интернете привело к тому, что, как отметил Касперский в одном из заявлений 2007 года, «в связи с этим людей,

занимающихся преступным «творчеством» и, соответственно, их творений – например, таких, как черви Slammer, Sasser или Mydoom, становится все меньше. Их нишей остаются, так называемые, «концептуальные» вирусы в пока еще не криминализированных зонах. Сейчас практически исчезли глобальные инциденты: многие виновники эпидемий прошлых лет обнаружены или изолированы от общества, а новые не стремятся составить им компанию» [6]. В результате резко выросло качество и количество локальных вредоносных программ, нацеленных на конкретную выгоду. Следуя императиву увеличения наживы, компьютерный андеграунд, – мозаика «из бесчисленного множества субкультур, реализующих себя в киберпространстве глобальной сети» [7], – претерпел существенные изменения: хакеров-исследователей, санитаров, любителей-коллекционеров вирусов и прочих «идеалистов» потеснили жесткие прагматики, тесно связанные с криминалом (крэкеры, пираты, вирмейкеры, кардеры, фрикеры).

В последующие годы киберпреступность в РФ как чрезвычайно прибыльная и в наименьшей мере подвергнутая риску наказания отрасль криминального бизнеса продолжала интенсивно развиваться: росло число спам-атак (по их числу наша страна еще в 2007 году вышла на второе место в мире после США), формировались новые генерации полиморфных вирусов (так, российской хакерской группировкой «Желатин» был создан и запущен в сеть высокоэффективный одноименный вирус, получивший на Западе наименование Storm Worm); участились случаи похищения паролей к онлайн-играм и виртуальной собственности для последующей их перепродажи или выкупа легитимным владельцем [8].

На последнем моменте хотелось бы остановиться подробнее. Представляется весьма знаменательным фактом то, что киберкультура, рожденная некогда в недрах компьютерного подполья, – вспомним, что первые компьютерные игры возникли на рубеже 60–70-х годов прошлого века среди первопроходцев киберпространства, энтузиастов открытия нового культурного локуса (студентов и молодых сотрудников Массачусетсского технологического института, Стэнфордского и Калифорнийского университетов) – не получила, в конце концов, иммунитета ни против коммерциализации, ни против криминализации, причем инициаторами того и другого процессов являются члены того же киберподполья. Данный факт, безусловно, свидетельствует об исчерпанности того этического потенциала бескорыстия, взаимопомощи и доверия, которые некогда сплачивали этот киберпротезированный локус контркультуры. Киберпреступность в сфере игрового бизнеса явно наращивает обороты. Так, в 2010 году «жертвой хакеров стала японская корпорация Sony. В результате атаки были похищены личные данные, в том числе номера кредитных карт, всех 77 млн. пользователей сервиса Playstation Network. Предварительный ущерб оценивается в 1,25 млрд. долларов» [9].

Более того, трудно оценивать иначе, чем проявление последовательной деградации криминализирующегося киберподполья его сознательное паразитирование на интернетизации социума, в конечном счете, им же – в лице компьютерного авангарда контркультуры – инициированного. Как отмечают исследователи, «масса новых сервисов, доступных через Интернет, и миллионы желающих этими сервисами пользоваться способствуют успеху киберпреступности», выделяя как наиболее уязвимые для атак такие области, как интернет-деньги, интернет-банкинг, удаленные хранилища данных в сфере финансовой, конфиденциальной и личной информации, онлайновые биржевые агентства и т.д. [10].

Ил. 3.

Прогрессирующая виртуализация социума, превращение Сети в базовое средство социально-культурной деятельности индивида, иными словами, становление общества web. 2.0, открыло перед преступниками новое поле деятельности. Социальные сети, блоги, форумы, wiki-ресурсы, твиттер – «все эти легкие в загрузке и публикации технологии обмена информацией делают его участников уязвимыми для заражения вредоносными программами» [10]. Причем тенденция эта – общемировая.

По данным Центра по обеспечению защиты от вредоносного программного обеспечения компании Майкрософт (Microsoft Malware Protection Center (MMPC), «объем фишинга[2] с использованием социальных сетей возрос с 8,3% от общего уровня использования фишинга в январе до 84,5% в декабре 2010-го.

Популярность сайтов социальных сетей открыла киберпреступникам широкие возможности, позволив им привлечь не только ничего не подозревающих пользователей, но также их друзей, коллег и членов семьи за счет персонализации. Эти методы добавляют к уже существующему списку техник социальной инженерии такие методы, как финансовые и продуктовые продвижения в электронной почте и службах мгновенных сообщений с целью вымогательства денег или обмана пользователей, вынуждающего их скачивать вредоносные файлы» [9].

Взрывообразный рост числа атак на пользователей популярных социальных сетей – один из актуальных трендов современной киберпреступности в РФ наряду с усложнением

[2] Фишинг (от англ. fishing – ловить рыбу, выуживать) – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей (паролям и логинам).

вирусных технологий, ростом числа ботнетов[3] с гибкой системой управления и криптографической защитой коммуникации, распространением все более разнообразных видов интернет-мошенничества, специализацией рынка производителей и потребителей киберкриминальных услуг [10]. Теневое подполье глобальной электронной цивилизации – столь же глобальная «сложная и мощная вирусная «экосистема» с разделением труда, состоящая из заказчиков и исполнителей заказов» [11], специализацией по разным странам и регионам мира. В киберкриминальном разделении труда РФ, увы, также занимает свою нишу: если по «количеству создаваемого вредоносного программного обеспечения мировым лидеров стал Китай, то по сложности и «инновационности» программ на первом месте – российские хакеры и вирусописатели» [11]. Экстерриториальность сети и анонимность (по желанию) интернет-пользователей предельно затрудняют локализацию киберпреступности. И хотя, как считают аналитики в сфере информационной безопасности, «Россия занимает 3-е место в мире по количеству атак в Интернете» [9], удельный вес «русской» киберпреступности в общемировом ее обороте довольно высок.

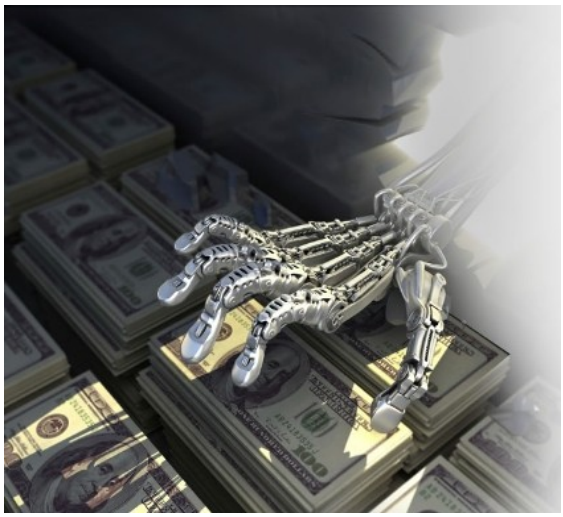
В 2011 году эксперты лаборатории компьютерной криминалистики российской компании Group-IB подготовили комплексный отчет: «Русский» рынок компьютерных преступлений в 2011 году: состояние и тенденции» [12]. Интересная новация аналитиков компании – разграничение «русского» и российского рынков современной киберпреступности. По их мнению, «русский» рынок киберпреступности представляет собой рынок компьютерных преступлений, совершаемых как гражданами РФ, так и гражданами стран СНГ и Прибалтики, а также гражданами других стран мира, но являющимися выходцами из стран бывшего СССР. Российский рынок является составной частью «русского» и представляет собой рынок компьютерных преступлений, совершаемых исключительно гражданами РФ» [12, с. 4].

Оценивая годовой финансовый оборот мирового рынка компьютерных преступлений в 7 млрд. долларов, эксперты Group-IB полагают, что на долю российского сегмента рынка из этой суммы приходится 1,3 млрд. долларов, в то время как общий доход «русского» рынка компьютерных преступлений составил сумму, превышающую первую почти в два раза. Иначе говоря, находясь территориально в различных регионах и совершая свои атаки по всему миру, «русские» хакеры заработали в 2010 году около 2,5 млрд. долларов» [12, с. 4].

---

[3] Ботнет (англ. «botnet» от «robot» и «network») – компьютерная сеть с программным обеспечением, работающим в автономном режиме. Используется для рассылки спама, атак на отказ в обслуживании, поиска конфиденциальной информации.

Стремительный рост киберпреступности в стране отмечают и правоохранительные органы. По данным Управления «К» МВД России, «за первые месяцы 2011 года количество киберпреступлений увеличилось на 95% по сравнению с аналогичным периодом прошлого года» [9], причем подавляющее большинство зафиксированных преступлений было связано с онлайн-торговлей. Аналитики компании Group-IB прогнозируют, что в 2011 году «русские» хакеры заработают около 3,5 млрд. долларов, а в 2013 году удвоят данный показатель. Приблизительно половина доходов «русского» сегмента рынка компьютерных преступлений будет приходиться на долю российских злоумышленников» [12, с. 4].



Ил. 4.

К числу наиболее распространенных в 2010 году преступлений «русских» хакеров аналитики лаборатории компьютерной криминалистики компании Group-IB относят: рост числа и сложности распределенных атак отказа обслуживания, направленные атаки на финансовый сектор и рост инцидентов в системах дистанционного банковского обслуживания, взрывообразный всплеск случаев смс-мошенничества на территории стран СНГ; использование приемов социальной инженерии для хищения персональной и конфиденциальной информации (через социальные сети и блоги), а также с целью интернет-мошенничества; целевые атаки на объекты критической инфраструктуры.

Современный всплеск киберпреступности, полагают специалисты, спровоцирован группой факторов: ростом степени профессионализации хакеров, затрачивающих значительные ресурсы «для совершенствования преступных схем, методов и инструментов» [12, с. 6]; расширением криминального рынка компьютерных услуг за счет появления новых участников, снижением цен на востребованные услуги; ростом внутреннего рынка киберпреступности, так называемой Cybercrime to Cybercrime или «киберпреступности в квадрате», когда злоумышленники заказывают услуги у своих же коллег; переход на сверхмонетизацию. Если «период 2003–2009 был знаковым по переходу киберпреступности на 100% монетизацию ее деятельности» [12, с. 6], то сейчас мошенники изыскивают всевозможные новые методы получения сверхприбыли.

Рост «русской» киберпреступности кроме того питают и такие факторы, как слабость законодательства и правоприменения в странах постсоветского пространства, высокий уровень технического образования, языковая общность; экономическая

нестабильность, когда далеко не все выпускники технических вузов могут найти достойную работу по специальности. К тому же типовые цены на криминальные онлайновые услуги на постсоветском пространстве чрезвычайно низки в сравнении с общемировыми. Так, если стандартная цена на продажу 1000 «загрузок» («зараженных» компьютеров) в США составляет 100–140 долларов, в Европе – 70–130 долларов, то в России она не превышает 20–40 долларов [12, с. 12].

Говоря о криминализации современного отечественного компьютерного андеграунда, не стоит, конечно, считать ее тотальной. В конце концов, компьютерное подполье – это и российский Фидонет[4] с пятьюдесятью тысячами пойнтов и числом пользователей, как минимум, в 5–10 раз больше (и больше, чем количество членов «сети друзей» во всем остальном мире [13]); это и сотни ежегодно рекрутируемых юных компьютерных фанатов; «бескорыстных душ», пополняющих субкультуры подполья, до взросления и окончательного перехода в лоно легальных социально-культурных практик. Кстати, как известно, в Фидонете практически нет преступности. Но Фидонет – уникальная коммуникативная модель, некоммерческий автономный оффлайновый ресурс, где нет анонимности, где даже некорректные высказывания безжалостно модерируются в соответствии с добровольно принятым этическим кодексом. Не обладая безграничными коммуникативными возможностями Интернета (в первую очередь гипертекстовыми ссылками), Фидонет – заповедник бескорыстия и дружелюбия киберкультуры 1979–1980-х годов – год за годом безжалостно оттесняется своим противником в некое субкультурное гетто, по большому счету сохранившее значимость лишь в постсоветском киберпространстве.

Большинство аналитиков считает качественный и количественный рост преступности в Сети одним из основных факторов, – наряду с «цифровым неравенством» между бедными и богатыми странами, технологическим диктатом США в сфере информационных технологий, недостаточным финансированием новаторских «прорывных» разработок в этой области и т. д. – ставящих под угрозу будущее Интернета. Так, в опубликованном в августе 2010 года прогнозе развития Интернета до 2025 года, подготовленном компанией Cisco и подразделением глобальных бизнес-сетей консалтинговой фирмы Monitor Group, растущая криминализация Сети признается одним из серьезнейших неблагоприятных факторов ее дальнейшей эволюции. Один из четырех альтернативных сценариев дальнейшего развития Интернета, выдвинутых в прогнозе, не случайно носит название «Неуверенный рост» (Insecure Growth) и описывает возможную в

[4] Подробнее о Фидонете см.: *Савицкая Т.Е.* Из истории компьютерного андеграунда: эпоха BBS и Фидонета. Часть II // Культура в современном мире. – 2011. – Вып. № 3 [Электронный ресурс]. – Режим доступа: http://infoculture.rsl.ru

будущем ситуацию, когда «борьба с кибертеррором и киберпреступностью становится затяжной, дорогостоящей, из-за низкой отдачи не вызывающей энтузиазма, во многом похожей на старую войну с наркотиками» [14]. Вал киберпреступности (непрестанные вирусные атаки, кража кредитных карт, взлом электронной почты, всевозможные виды интернет-мошенничества, электронный шантаж, засилье спама) заливает Сеть, превращая ее в опасное и некомфортное место, от посещения которого массовый пользователь старается воздерживаться.

Но это – о будущем, о далеком 2025 годе; один из вариантов прогнозируемого состояния Сети, который может и не осуществиться. В настоящем же – поражает скепсис и крайняя осторожность киберпрогнозов, рассчитанных на ближайшее время.

Так, Наталья Касперская, прибывшая в мае 2011 года в Париж для участия в международном интернет-форуме, где она представляла «Лабораторию Касперского» и InfoWatch, заявила: «Количество вирусов растет экспоненциально. Если несколько лет назад их насчитывалось несколько десятков тысяч, то в 2010 году мы зарегистрировали уже порядка 4 миллионов различных вирусов. Ситуация осложняется тем, что зачастую вследствие использования хакерами заграничных серверов просто невозможно проследить источник распространения вредоносных программ или исполнителей кибератак. Общая раскрываемость преступлений в киберпространстве низкая – не более 5 процентов. Стоит учитывать, что о многих «утечках» просто не сообщается. То, что предается огласке, – это только видимая сторона айсберга» [9].

По мнению экспертов лаборатории компьютерной криминалистики компании Group-IB, «ужесточение наказаний, активизация межгосударственной работы, привлечение к сотрудничеству отраслевых ассоциаций и популяризация фундаментальных политик информационной безопасности будут способствовать снижению современных темпов роста «русского» рынка киберпреступности» [12]. Разумеется, комплексные меры по обузданию киберпреступности (включая, например, введение международного Интернетпола) необходимы, но в заключение статьи хотелось бы задуматься над вопросом: почему же Сеть не стала электронным раем, зоной свободы и сотрудничества, местом безопасного самопроявления всех и каждого? Почему не сбылись мечты отцов-основателей Интернета; почему превратился он в карикатурный слепок современного общества, укрупнивший не только его достоинства, но и также все пороки?

С точки зрения культуролога, причина нравственно-этической индифферентности Интернета, приведшей, в частности, к криминализации киберподполья, заключается не столько в нынешней массовости Сети, привлекающей как «добрых», так и «злых» пользователей, сколько в том, что Интернет как базовый социальный институт

глобального общества постмодерна изначально находится вне рамок какого бы то ни было культурного канона. Сейчас можно уже, кажется, констатировать практически полное иссякновение морального импульса контркультуры, одушевлявшего некогда первоначальные протоструктуры Сети. Интернет сам стал средоточием нового Истеблишмента. Но без существенных морально-правовых коррекций (например, весомого ограничения анонимности пользователей) он вряд ли принесет счастливое будущее.

Список литературы.

1. Прохоров. А. Интернет в цифрах и фактах. – [Электронный ресурс]. – Режим доступа: URL: http://www.compress.ru/Archive/CP/2006/2/1/ (дата обращения: 10.03.2011).

2. Russia Has World's Most Engaged Social Networking Audience. – [Электронный ресурс]. – Режим доступа: URL: http://www.comscore.com (дата обращения: 13.07.2011).

3. Статистика пользователей Интернета. – [Электронный ресурс]. – Режим доступа: URL: http://www.bloxpot.net/2010/10/statistica-interneta.html (дата обращения: 15.11.2011).

4. Исследование компьютерного андеграунда на постсоветском пространстве. – [Электронный ресурс]. – Режим доступа: URL: http://bugtrag.ru/library/undeground/research.html (дата обращения: 24.10.2011).

5. Statistics [Электронный ресурс]. – Режим доступа: http://www .lifejournal.com/stats.html (дата обращения: 27.10.2011).

6. Касперский Е. Компьютерный андеграунд переходит в лигу «профессионалов». – [Электронный ресурс]. – Режим доступа: URL: http://www.cnews.ru/reviews/free/security/2007/articles/underground. (дата обращения: 07.11.2011).

7. Анализ формирования компьютерного андеграунда в контексте современной киберкультуры – [Электронный ресурс]. – Режим доступа: URL: http://pelevin.su/localnews.php?n=119 (дата обращения: 17.11.2011)

8. Компьютерный андеграунд 2008: вред за деньги – [Электронный ресурс]. – Режим доступа: URL: http://www.webplanet.ru/company/security/2008/02/19/kasperskiy.html (дата обращения: 20.11.2022).

9. Киберпреступность. За год число киберпреступлений в Рунете выросло вдвое [Электронный ресурс]. – Режим доступа: URL: http://itgator.ru/tag/kiberprestupnost/ (дата обращения: 16.11.2011).

10. Киберпреступность пришла, чтобы остаться [Электронный ресурс]. – Режим доступа: URL: http://www.itsec.ru/newstext.php?news=id=4978. (дата обращения: 10.10.2011).

11. «Компьютерный андеграунд»: итоги и прогнозы [Электронный ресурс]. – Режим доступа: URL: http://www.pcweek.ua/themes/detail.php?ID=122493&THEME_ID. (дата обращения: 18.10.2011).

12. «Русский» рынок компьютерных преступлений в 2010 году: состояние и тенденции. – М.: 2011.

13. Fido-Statistik – [Электронный ресурс]. – Режим доступа: URL: http://www.was-ist-fido. (дата обращения: 23.03.2011).

14. The Evolving Internet. Driving Forces, Uncertainties and Four Scenarios to 2025 – [Электронный ресурс]. – Режим доступа: URL: http://newsroom.cisco.com. (дата обращения: 25.09.2011).

Сведения об использованных иллюстрациях:

1. [Электронный ресурс]. – Режим доступа: URL: http://img576.imageshack.us/img576/3626/image73c.jpg (дата обращения: 21.02.2012).

2. [Электронный ресурс]. – Режим доступа: URL: http://vesti.kz/internet/76440/ (дата обращения: 21.02.2012).

3. [Электронный ресурс]. – Режим доступа: URL: http://cassandra.com.ua/index23-4.php (дата обращения: 21.02.2012).

4. [Электронный ресурс]. – Режим доступа: URL: http://fc02.deviantart.net/fs21/f/2007/232/2/a/fish_eye_by_ssecret.jpg (дата обращения: 21.02.2012).

5. [Электронный ресурс]. – Режим доступа: URL: http://activerain.com/blogsview/1978111/how-to-prevent-cyber-crime-plug-the-cyber-leaks- (дата обращения: 21.02.2012).

Источник: ***Культура в современном мире. — 2012. — № 1. — [Электронный ресурс].*** — Режим доступа: ***URL:*** http://infoculture.rsl.ru