Правовые основы безопасности информационного общества

Яковенко А.А.[*]

Особенности развития процессов глобализации в условиях современной действительности обусловлены переходом общества от индустриального к информационному[1]. Мы живем в век бурного технического прогресса, современных стремительно развивающихся и постоянно обновляемых высоких технологий, информационно-компьютерных систем[2]. Повсеместное внедрение новейших информационно-коммуникационных технологий (ИКТ) формирует новые потенциалы для стран с транзитивной экономикой. Это касается и самого государства, и его политики, а также общества и сознания его индивидов.

Президент Республики Узбекистан И.А. Каримов отмечает, что в качестве важнейшей составляющей процессов формирования основ гражданского общества мы рассматриваем обеспечение либерализации средств массовой информации, ускоренное развитие информационно-коммуникационной сферы[3].

Тем не менее, несмотря на множество положительных моментов ИКТ в современном мире, важно учитывать тот факт, что их совершенствование способствует не только укреплению общественных связей, но и появлению ранее неизвестных источников риска и опасности.

Получая несомненные преимущества от использования новейших информационных систем, построенных на основе глобальных компью-

---

[*] Яковенко А.А. – юрист-международник, Национальный университет Узбекистана.

[1] О развитии информационного общества см. подробнее: Negroponte N. Being Digital // New Times. – 1988. – October; Gates B. The Road Ahead. – Harmondsworth: Penguin, 1995; Dertouzous Michel L. What will be: How the New World of Information will Change our Lives. – Piaktus, 1997. Webster Frank. Theories of the Information Society. – London: Routledge, 2002.

[2] Каримов И.А. Стратегия реформ – повышение экономического потенциала страны / Доклад Президента Республики Узбекистан Ислама Каримова на заседании Кабинета Министров, посвященном итогам социально-экономического развития страны в 2002 году и основным направлениям углубления экономических реформ на 2003 год. http://www.press-service.uz

[3] См. подробнее: Каримов И.А. Выступление на торжественном открытии ежегодного заседания совета управляющих Европейского банка реконструкции и развития. Избранный нами путь – это путь демократического развития и сотрудничества с прогрессивным миром. – Т.: Узбекистан, 2003.

терных сетей, Республика Узбекистан также постепенно входит в определенную зависимость от их эффективного функционирования. Это обстоятельство, по нашему мнению, заставляет вырабатывать новые правовые методы защиты интересов общества и государства.

Анализ глобальных информационных отношений свидетельствует об определенном уровне их опасности. Так, согласно данным ФБР, финансовые потери 494 опрошенных компаний в 2004 году составили 141 496 560 долл. США[4]. Общественно опасная деятельность в Сети получает все большее распространение. К примеру, настоящий киберджихад за Кашмир ведут друг против друга хакеры Пакистана и Индии. Пакистанские хакеры взламывают веб-сайты индийских государственных учреждений. В свою очередь, индийская хакерская группа (Indian Snakes) в качестве «виртуальной мести» распространила сетевой червь Yaha-Q. Главной задачей Yaha-Q стало совершение DDOs-атак на некоторые пакистанские ресурсы, среди которых – интернет-провайдеры, сайт фондовой биржи в Карачи (Karachi Stock Exchange) и правительственные ресурсы. Помимо этого в начале 2003 года объявил о себе как о новой террористической организации «Арабский Электронный Джихад» (AEJT) под новым для террористов лозунгом: поставить на колени Интернет. Организация AEJT заявила о том, что собирается уничтожить все израильские и американские веб-сайты, а также «все другие неугодные ей сайты»[5].

Далее, в августе 2003 года произошло обвальное отключение электричества в США, в результате которого только предварительный ущерб исчислялся в 2-6 млрд. долл. В ходе расследования этой аварии появились новые факты, из которых следует, что именно сбои в компьютерных системах энергосетей стали основной причиной чрезвычайного происшествия. В день каскадного отключения червь Blaster забил каналы, которые использовались для связи между диспетчерскими центрами. В результате время передачи данных значительно возросло и персонал не смог предотвратить развитие каскада. А уж кто больше претендует на роль главного подозреваемого – сетевой червь

[4] 2004 CSI/FBI Computer Crime and Security Survey Continue but Financial Losses are Down // http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf. По данным же Украинского антивирусного центра, разработчика комплексных систем антивирусной защиты, потери от вирусных атак в первом полугодии 2004 г. составили 290 млн. гривен (около 45 млн. евро). По сравнению с аналогичным периодом 2003 года убытки выросли на 30%. http://www.crime-research.ru/news/30.07.2004/1320

[5] См. подробнее: http://www.crime-research.ru

Blaster (Lovsan) или террористическая группировка «Бригады Абу-Нафса», которая входит в сеть «Аль-Каиды», – вряд ли будет установлено в ближайшее время[6].

По данным исследования, проведенного исследовательским институтом United States Institute for Peace (USIP), Всемирная Сеть является «идеальной средой для деятельности преступников, поскольку доступ к ней крайне легок, в ней легко обеспечить анонимность пользователей, она никем не управляется и не контролируется, в ней не действуют законы и не существует полиции». Если в 1998 году примерно половина из 30 организаций, которых США причисляли к террористическим, обладали своими сайтами, то ныне в Сети представлены абсолютно все известные террористические группы, которые публикуют свои материалы, по меньшей мере, на 40 различных языках. Террористические группы создают и многоязычные сайты, дабы оказать влияние на людей, которые напрямую не вовлечены в конфликт. К примеру, баскская террористическая организация ETA предлагает информацию на испанском, немецком, французском и итальянском. Шри-ланкийская группировка «Тигры Освобождения Тамил Илам» публикует свои материалы на английском, японском и итальянском, Исламское движение Узбекистана – на узбекском, арабском, английском и русском[7].

В такой ситуации требуется правовое регулирование глобальных информационных отношений в целях всемерной защиты их субъектов. Мировым сообществом и отдельными государствами были предприняты меры по формированию законодательной базы по обеспечению безопасности формирующегося информационного общества.

Так, Генеральная Ассамблея ООН приняла в декабре 1998 года резолюцию, касающуюся киберпреступности, кибертерроризма и кибервойны. Резолюция 53/70 призывает государства-члены информировать Генерального секретаря ООН о своих взглядах и оценках относительно проблем информационной безопасности, определения основных понятий, связанных с информационной безопасностью и развитием международных принципов, улучшающих глобальное информационное пространство и телекоммуникации и помогающих сражаться с информационным терроризмом и преступностью[8].

---

[6] Голубев В. Организационно-правовые аспекты противодействия компьютерной преступности и кибертерроризму. – 2004. http://www.crime-research.ru

[7] http://www.usip.org

[8] http://www.un.org

Помимо этого ведутся законодательные наработки и в развитых странах. К примеру, в июле 1996 года Президент США Б. Клинтон объявил о формировании Президентской комиссии по защите критических инфраструктур (PCCIP). В заключительном отчете, изданном в октябре 1997 года, комиссия сообщила, что "угрозы критическим инфраструктурам реальны и, через взаимосвязь и взаимозависимость, инфраструктуры могут быть уязвимы для новых способов нападения. Умышленная эксплуатация этих слабых мест может иметь серьезные последствия для экономики, безопасности и жизни. PCCIP также отметила, что киберугрозы изменили обстановку. "В прошлом мы были защищены от нападений врага на инфраструктуры широкими океанами и дружественными соседями. Сегодня эволюция киберугроз разительно изменила ситуацию. В киберпространстве национальных границ нет. Электроны не остановишь для того, чтобы проверить паспорт. Потенциально опасные кибернападения могут быть задуманы и подготовлены без обнаружения подготовки. Они могут незримо разведываться, тайно репетироваться, а потом быть воплощены в жизнь за минуты или даже за секунды, без того, чтобы идентифицировать нападающего или установить его местоположение". Рекомендации PCCIP привели к изданию указа президента № 63, которым были созданы: Национальный центр защиты инфраструктур (NIPC), Офис безопасности критических инфраструктур (CIAO), Национальный совет защиты инфраструктур (NIAC) и частные Центры распределения и оценки информации (ISACs).

В январе же 2001 года Советом национальной безопасности был принят Национальный план защиты информационных систем. Мало того, Сенат США 13 сентября того же года не только одобрил законопроект Combating Terrorism Act of 2001, который разрешил использование Федеральным бюро расследований применение системы Carnivore[9], но и уве-

[9] Система тотального наблюдения (также известная, как DCS1000), предназначенная для военного разведывательного агентства. Надо сказать, что системы такого рода разрабатываются не только в США. Аналогичная система разрабатывается в рамках проекта TREVI (Text Retrieval and Enrichment for Vital Information), который предназначен для «прослушивания» и анализа телекоммуникационных каналов стран Европейского союза. Разработка этой системы была одобрена еще 23 ноября 1995 года всеми членами ЕС. При этом ЕС принял решение направить письмо различным международным организациям, занимающимся вопросами телекоммуникаций (например, ISO и ITU), с рекомендацией учета положений проекта TREVI при разработке требований к телекоммуникационному оборудованию и услугам. Лукацкий А.В. Кибертерроризм: за и против. http://www.crime-research.ru

личил ассигнования на следующий год на развитие данной системы[10].

В 2002 году Пентагон предоставил одному из крупнейших научно-исследовательских учреждений США – университету Carnegie Mellon 35,5 млн. долл. на проведение исследований в области борьбы с компьютерной преступностью. Пятилетний грант предусматривает развитие идентификационных технологий, призванных оградить пользователей Интернета от несанкционированного доступа к их конфиденциальным данным[11]. Далее в специально созданном при университете Центре компьютерной безопасности и защиты коммуникаций ведутся научно-исследовательские работы по созданию элементов искусственного интеллекта, обеспечивающих защиту информации от атак со стороны хакеров в автоматическом режиме без участия человека. Кроме того, активно проводятся изыскания с целью изучения возможностей использования индивидуальных особенностей пользователя: его подписи, отпечатков пальцев, внешности и голоса для пресечения несанкционированного доступа к данным. Как полагают ученые, в дальнейшем для защиты информации от компьютерных террористов будет применяться симбиоз этих технологий[12].

В Великобритании вступило в действие законодательство, в соответствии с которым, в случае взлома хакерами компьютерной системы, обеспечивающей национальную безопасность страны, а также попыток с их стороны каким-либо образом оказать воздействие на государственные структуры или угрожать обществу, они могут быть обвинены в терроризме со всеми вытекающими последствиями[13].

В странах континентальной Европы идут аналогичные процессы. В разряд приоритетных выдвигается вопрос правовых и организационных механизмов регулирования использования компьютерных сетей. Первым международным соглашением по юридическим и процедурным аспектам расследования и криминального преследования киберпреступлений стала Конвенция о киберпреступности, принятая Советом Европы 23 ноября 2001 г.[14]. Конвенцией предусматриваются ско-

[10] Там же.

[11] См. подробнее: Wilkinson P. The Laws of War and Terrorism // TheMorality of Terrorism / Ed. by D. Rappoport, Y. Alexander. – N.-Y.: Columbia University Press, 1989.

[12] Малышенко Д.Г. Противодействие компьютерному терроризму – важнейшая задача современного общества и государства. - ВНИИ МВД России. http://oxpaha.ru/view.asp?13341

[13] Там же.

[14] http://www.crime-research.org/library/cybercrime-convention.doc

ординированные на национальном и межгосударственном уровнях действия, направленные на недопущение несанкционированного вмешательства в работу компьютерных систем.

Также немаловажной проблемой является и необходимость разрешить вопрос о контроле над информацией, распространяемой в Интернете. Данная проблема носит комплексный, многоплановый характер. С одной стороны, очевидно, что принятое в цивилизованных странах в качестве аксиомы право человека на свободный доступ к информации является одним из краеугольных камней фундамента, на котором зиждется свободное общество. С другой – не секрет, что права и свободы, предоставленные таким обществом без ограничений всем составляющим его индивидуумам, в некоторых случаях с успехом используются преступниками, которые осуществляют обмен информации, координацию и пропаганду своих действий, пользуясь для этого возможностями сети[15].

По нашему мнению, следует выработать систему признаков интернет-ресурсов, пропагандирующих ксенофобию, расовую и религиозную нетерпимость, и на ее основе создать единый перечень подобных интернет-ресурсов в целях координации действий по их нейтрализации.

Таким образом, можно констатировать, что угроза безопасности информационному обществу в настоящее время является очень сложной и актуальной проблемой, причем она будет нарастать по мере развития и распространения ИКТ.

Деятельность по противодействию киберугрозе должна носить системный и комплексный характер. Необходимо строить эту работу на базе четкого взаимодействия всех правоохранительных органов, внедрения эффективных методов раскрытия и профилактики такого вида преступлений, а также совершенствования правовых норм.

Очевидно, что ни одно государство сегодня не в состоянии противостоять этому злу самостоятельно. Такая борьба не может быть уделом отдельно взятых государств, поэтому необходимо обеспечить взаимодействие спецслужб, включая национальные службы безопасности и специальные подразделения по борьбе с терроризмом на национальном, региональном и международном уровнях.

Поскольку современная компьютерная преступность представляет собой существенную угрозу, необходимо закрепить на законодательном уровне обязанность государственных и частных структур по при-

[15] Голубев В. Проблемы противодействия …

нятию технических мер, обеспечивающих защиту компьютерных сетей как одного из наиболее уязвимых элементов современного технологически зависимого общества.

Отдельного внимания в плане формирования общей модели противодействия киберпреступности заслуживают примыкающие к программно-техническим сервисам вопросы, связанные с выработкой системы в организации аудита новых технических средств и программного обеспечения. Настоятельная потребность в аудите и сертификации аппаратных средств объясняется возможностью их использования в национально значимых компьютерных системах.

Помимо прочего, требуется проведение научных исследований в области разработки единого понятийного аппарата[16]. Необходима проработка и корректировка законодательных, нормативных и правовых документов в отношении этого вида преступления, в том числе регламентирующих международную деятельность. Важнейшее значение имеют научные работы в области создания современных технологий обнаружения и предотвращения сетевых атак и нейтрализации криминальных воздействий на информационные ресурсы. Очевидно, что все это невозможно без совершенствования многоуровневой системы подготовки кадров в области информационной безопасности.

Реализация указанных мер позволит в конечном итоге сформировать эффективную систему защиты информационного общества от глобальных проблем киберпреступности.

---

[16] О понимании значимости, внимании к этой проблеме и попытках выработки такой системы мер на концептуально-теоретическом и практическом уровнях свидетельствуют, например, неоднократные обсуждения вопросов экстремизма на сетевой среде на межведомственном, междисциплинарном семинаре по научным проблемам информационной безопасности, проводимом в Московском университете под эгидой Совета Безопасности РФ и МГУ, доклады на российско-американском семинаре «Высокотехнологичный терроризм», прошедшем Москве в июне 2001 г., а затем, его продолжении в декабре того же года в США, проводившемся Российской академией наук совместно с Национальными академиями США. На этом семинаре (еще до трагических событий сентября 2001 г.) рассматривались потенциально возможные направления использования различных технологий в террористических целях, включая химическое и бактериологическое, ядерное и компьютерное (кибертерроризм), возможные сценарии их использования, а также системы мер, как стратегического, так и оперативно-тактического характера. См. подробнее: Высокотехнологичный терроризм. Материалы российско-американского семинара. Москва, 4-6 июня 2001 г., – М.: РАН, 2001. – 320 с.

Legal Foundation of the Security of Information-oriented Society (Summary)

*Yakovenko A.A.**

In the introduction the author points out that widespread application of modern information technologies enhances the development of the economy but simultaneously poses new threats and challenges to the society. This circumstance leads to the necessity of developing new legal methods for protection of the state interests and the interests of the society.

The author states that according to the research done by the United States Institute for Peace (USIP) the Internet is a perfect environment for the criminal activity as access to it is relatively easy, laws do not function there, there is no police. In this situation it is clear that global relations in the aspect of information should be governed by law for the purposes of protection of its subjects. International community and states individually had undertaken several steps towards the elaboration of legal norms to provide security of the emerging information-oriented society. For example, the UN General Assembly adopted the Resolution 53/70 concerning cyber crimes, cyber terrorism and cyber war. Similar steps are also taken on the national level.

The other crucial issue in this sphere is the necessity of certain control over the information on the Internet. This is a controversial issue due to the right of an individual to a free access to the information. The author suggests creating the criteria for distinguishing Internet resources advocating xenophobia, racial and religious intolerance, etc.

Thus the author comes to a conclusion that the threat to information security is an acute and complicated problem which cannot be resolved by states separately and requires their cooperation. Further the author focuses on the measures of combating cyber crimes and securing the information. The implementation of these measures, in author's opinion, will help to create an effective system of protection of the information-oriented society from the threats of cyber crime.

* Yakovenko A.A. – international lawyer, National University of Uzbekistan.