ГОСУДАРСТВО И ПРАВО, 2008, № 8, с. 82–85

РАЗВИТИЕ ИНФОРМАЦИОННО-ЭЛЕКТРОННЫХ СИСТЕМ КАК ОБЪЕКТ ПРАВОВОГО АНАЛИЗА В УСЛОВИЯХ НАРАСТАНИЯ УГРОЗЫ КИБЕРТЕРРОРИЗМА

© 2008 г. О. А. Степанов[1]

Начало XXI в. связано с развитием самой мощной в истории человечества информационно-технологической революции. Можно вслед за О. Шпенглером, Д. Беллом, Г. Гэлбрейтом, Э. Тоффлером, З. Бжезинским, Е. Масудой, П. Морелом, Д. Урсулом, А. Ракитовым, Ф. Фукуямой[2] и некоторыми другими называть наиболее развитые страны обществами "информации и услуг", "постиндустриальными", "сверхиндустриальными", "технотронными", "информационными", "информационно-индустриальными", но нельзя не замечать того, что для всех развитых современных обществ новые информационно-электронные технологии стали фундаментальной основой экономического, политического и социального развития.

Если результаты целенаправленной деятельности человека в области экономики, политики, общественного сознания, общественной и национальной безопасности, науки, опосредованные использованием вычислительных, телекоммуникационных, биоэлектронных и психокомпьютерных технологий, ассоциировать с развитием информационно-электронных систем (ИЭС), то такие результаты вполне могут рассматриваться в качестве ключевого фактора, определяющего характер жизнедеятельности современного общества в условиях нарастания угрозы кибертерроризма[3].

Под кибертерроризмом обычно понимают действия лица или группы лиц, направленные на устрашение людей, оказание давления на правительства и организации с целью создания атмосферы страха в обществе, навязывания им определенной линии поведения либо причинения существенного вреда посредством использования информационно-электронных сетей, систем или информационно-электронных данных. В этой связи важно обратить внимание на то, что идея безопасности, заложенная в Законе РФ "О безопасности" (1992 г.)[4], прежде всего соотносится с состоянием "защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз".

Вместе с тем, по мнению В.В. Серебрянникова, безопасность следует соотносить с деятельностью не только людей, общества, государства, но и мирового сообщества народов, связанной с выявлением (изучением), предупреждением, ослаблением, устранением (ликвидацией) и отражением опасностей и угроз, способных погубить их, лишить фундаментальных материальных и духовных ценностей, нанести неприемлемый (недопустимый объективно и субъективно) ущерб, закрыть путь для выживания и развития[5].

Такой подход к безопасности предполагает необходимость осуществления системных действий по локализации существующих и потенциальных угроз человеку, обществу, государству в условиях нарастания угрозы кибертерроризма, связанной с развитием ИЭС.

Новые мировые реалии, обусловленные уменьшением значения географических границ государств и национальной принадлежности личности, которые определяются развитием сети Интернет, не имеющей в правовом смысле теоретических аналогов, в значительной степени определяются тем, что число пользователей "всемирной паутины" с начала XXI в. увеличилось к началу 2007 г. более чем в три раза.

Данная информационно-телекоммуникационная инфраструктура в настоящее время вполне может характеризоваться как некое "технологическое ядро", обеспечивающее связь пользователей различных информационных сетей (локальных, межрегиональных, общенациональных) по всему миру.

Производство и управление, оборона и связь, транспорт и энергетика, финансы, наука и образование, средства массовой информации и туризм – все это уже в значительной степени зависит от интенсивности информационного обмена, полноты, своевременности и достоверности информации в Интернете, для подключения к которой необходимо иметь лишь компьютер, модем, необходимое программное обеспечение и осуществить умеренную плату за аренду линий связи. Вместе с тем феномен системы Интернет, требующий осмысления с правовых позиций заключается еще и в том, что с функционированием и развитием этой системы возникло не просто гигантское информационно-электронное пространство ("киберпространство"), спо-

[1] Профессор Академии управления МВД России, доктор юридических наук.

[2] *Гэлбрейт Дж.К.* Новое индустриальное общество. М., 1969; *Тоффлер Э.* Третья волна. М., 1999; *Masuda Y.* The Information Society as Post Industrial Society. World Future Society. Washington, 1983. P. 139; *Ракитов А.И.* Россия в глобальном информационном процессе и региональная информационная политика // Проблемы информатизации. 1993. № 1–2. С. 3–19; *Урсул А.Д.* На пути к информационно-экологическому обществу // Философские науки. 1991. № 5. С. 3–16; *Fukuyama F.* Our Posthuman Future. New York, 2002.

[3] По мнению Д.Б. Фролова, сотрудника Центра информационной безопасности ФСБ России, термин "кибертерроризм" появился в середине 80-х годов прошлого века в США для обозначения террористических действий в виртуальном пространстве.

[4] См.: Ведомости Съезда народных депутатов и Верховного Совета РСФСР. 1992. № 15. Ст. 769.

[5] *Серебрянников В., Хлопьев А.* Социальная безопасность России. М., 1996. С. 16.

собствующее образованию более взаимосвязанного мира, но и появились новые проблемы с точки зрения обеспечения безопасности человека, общества, государства. Так, например, развитие мирового информационно-электронного пространства сопровождается фактами целенаправленного негативного воздействия на сознание и психику человека.

Постепенно в обиход вводятся такие понятия, как "информационная война", "компьютерные войны", "кибервойны", "войска информационных технологий", "информационное оружие", которые связаны с возможностью психологического принуждения личности, вовлеченной в телекоммуникационный процесс, либо изменения жизненно важных для ее физического состояния параметров.

В частности, в Стэнфордском исследовательском институте США на протяжении более чем десяти лет с помощью компьютерных технологий проводятся эксперименты по достижению одними людьми целей за счет манипулирования другими, не подозревающими об этом. Такие технологии получили обобщенное название "психотронное оружие". В их рамках прорабатываются возможности незаметного для человека стирания информации в его сознании, добавление новой информации, заставляющей совершать те или иные поступки вплоть до самоуничтожения. Такое оружие поражает мозг человека, разрушает способы и формы идентификации личности, трансформирует память человека, создавая личность с заранее заданными параметрами[6]. Развязывание на базе реализации таких методов вооруженных конфликтов делает весьма проблематичным не только их удержание в локальных рамках, но и недопущение попадания "психотронного оружия" в распоряжение террористов.

Согласно директиве Министерства обороны США и директиве Комитета начальников штабов Вооруженных Сил США Т9 3600 от 1992 г., а также Меморандуму заместителей министра обороны и председателя Комитета начальников штабов США № 30 от 1993 г. ведение информационной войны связывается с действиями, предпринимаемыми для достижения информационного превосходства в рамках реализации национальной военной стратегии посредством поражения компьютерных систем и пользователей противника (при одновременном обеспечении безопасности и защиты собственной информации и информационных систем), в том числе путем реализации ультрамозгового контроля[7].

Такой контроль порою связан с возможностью кодировки пользователей путем электронного подбора цветовых сочетаний на экране монитора, ритмичного изменения масштаба изображения (частотного воздействия в диапазоне естественных ритмов головного мозга) либо его яркости, контрастности, которые не замечаются человеком на уровне сознания. В результате ультрамозгового вторжения появляется возможность корректировки поведения человека (вызова стресса, усталости, депрессии, дезинформации) в наиболее важных ситуациях. И даже если жертва воздействия психотронных технологий окажется устойчивой к включенной компьютерной сублимации (неосознанному восприятию), команде на самоубийство или убийство (ничего подобного не совершит), то все равно такое подсознательное воздействие заложит в мозг "мину" замедленного действия, разрушающую психику человека, создаст канал для зомбирования личности.

Следует принимать во внимание, что подобного рода угрозы психическому здоровью человека могут также проявляться при корректировке его интеллектуальных и мотивационных особенностей, в частности пропаганды насилия, жестокости и правового нигилизма. Компьютерный вирус такого типа, "выпущенный" из машины, способен перерождаться в "социальный вирус", опасность которого обусловливается серьезными изменениями в общественной ориентации. Возможность распространения таких вирусов позволяет по-новому рассматривать базовые причины фанатизма, одержимости, революций, войн и кибертерроризма[8].

В этой связи уместно привести высказывание одного из руководителей Пентагона: "Мы приближаемся к такой степени развития, когда уже никто не является солдатом, но все – участниками боевых действий. Задача теперь не в уничтожении живой силы, но в подрыве целей, взглядов и мировоззрения населения, в разрушении социума"[9].

В известном "плане Даллеса" еще в 1945 г. было заявлено, что "человеческий мозг, сознание людей способны к изменению. Посеяв там хаос, мы незаметно подменим их ценности на фальшивые и заставим в эти фальшивые ценности верить"[10].

В настоящее время категория "контролируемый хаос" все более активно применяется в США в политическом обиходе по отношению к другим странам.

По мнению американских специалистов, принципиальная новизна использования психокомпьютерных технологий в антигуманных целях состоит в том, что систему, на которую направлено воздействие таких технологий, не надо разрушать полностью, ее достаточно перепрограммировать, и она разрушит себя сама либо будет выведено из строя управление ее стратегическими компонентами[11]. "Информация – это новая монета в международной сфере, и Соединенные Штаты имеют лучшие возможности, чем любая другая страна, для того, чтобы усилить посредством информации свой потенциал твердой и мягкой силы", – отметил специалист в области стратегических исследований Э. Коэн[12]. Реализация планов США по созданию в первой четверти XXI в. глобальной инфраструктуры на базе новой мощной информационной супермагистрали (Next Generation Internet) допускает возможность применения такой системы для ведения информационных войн, в ходе ко-

[6] См.: *Лопатин В.Н.* Информационная безопасность России. Человек. Общество. Государство. СПб., 2000. С. 103.

[7] См.: там же. С. 99.

[8] *Абрамов В.А., Рысин Ю.С.* Информационно-психологические вирусы и телерадиовещание // Современное телевидение. Труды 11-й научно-практической конференции. Москва, 18–19 марта 2003 г. М., 2002. С. 7–8.

[9] См.: Новая газ. 2001. 8–11 июня.

[10] См.: Правопорядок. 2002. № 2. С. 3.

[11] В интервью агентству "Интерфакс" 28 сентября 2006 г. руководитель антитеррористического центра СНГ генерал-полковник Б. Мыльников обратил внимание на потенциальную угрозу взаимосвязи ядерного и кибертерроризма, связанную с применением компьютерных технологий в атомной энергетике и промышленности.

[12] См.: Наука и религия. 2001. № 5. С. 21.

торых прежде всего планируется подавлять работоспособность систем управления противника и воздействовать на его личный состав путем реализации ультрамозгового контроля, дистанционного изменения поведения человека[13]. В этих целях Пентагоном разработана программа по управлению общественным мнением и политиками в других странах, в рамках которой отрабатываются технологии телезомбирования людей путем использования "25-го кадра", "дельта-шумов" (программы МК – "Ультра" и "Дельта", направленные на ультрамозговой и дистанционный контроль поведения человека), воздействующих на психику человека и способных полностью изменять его мышление, программировать поведение, нарушать адекватность реакций (вплоть до блокирования сосудов головного мозга у операторов ЭВМ), прививать синдром зависимости.

Следует отметить, что исследования, связанные с психологической обработкой войск и населения, с идеологическими диверсиями и дезинформацией, пропагандой и распространением ложных слухов, с управлением индивидуальным и коллективным поведением, с искажением получаемой руководителями информации, проводятся в Германии, Австрии, Франции, Италии, Японии, Израиле, Китае и некоторых других странах[14].

В рамках анализа при выделении потенциально-опасных типов ИЭС соответствующей правовой оценки заслуживают и существующие возможности вторжения в частную жизнь человека, обусловленные использованием электронных баз персональных данных. В ряде государств (Дании, Исландии, Норвегии, Швеции, Финляндии, Голландии и др.) гражданам с рождения в обязательном порядке присваиваются единые идентификационные номера, которые вводятся в электронные банки и фигурируют во всех их личных документах до самой смерти. При этом структура информационных систем, применяемых для таких целей, носит интегрированный характер, т.е. позволяет не просто накапливать информацию, но и оперативно анализировать, связывать данные, классифицировать их по заданным параметрам в интересах соответствующих государственных органов.

Созданная в США многоканальная система электронных учетов населения содержит такие данные, что фактически отпадает необходимость во внутренней паспортизации (в течение жизни на гражданина заводится от 50 до 100 электронных досье на федеральном уровне, на уровне штатов и нижестоящих уровнях). Результатом такого развития общества является хранение в электронных банках данных информации на сотни миллионов человек.

В России завершено создание многоуровневой системы интегрированных банков данных органов внутренних дел, концентрирующих информацию о лицах, представляющих интерес для сотрудников органов внутренних дел, вещах и предметах, имеющих отношение к преступлениям, об организованных преступных группах, а также сведения управленческого характера. На базе этих программно-технических комплексов развернуты работы по информационному обеспечению не только органов внутренних дел, но также налоговых и таможенных органов России.

Осуществление теоретико-правовой оценки функционирования и развития информационно-электронных систем, связанных с электронными учетами, является актуальным не только из-за углубления процесса глобализации, предполагающего интеграцию национальных электронных ресурсов в единые международные банки данных, но и вследствие возможных утечек конфиденциальных данных из ИЭС[15]. При этом особенности телекоммуникационного доступа к информационно-электронным системам, связанным с управлением и контролем различными объектами, дают основания ожидать принципиально новых проявлений не только шантажа, вымогательства, но и кибертерроризма.

Серьезнейшую опасность представляет перехват террористами управления, например, орбитальной космической группировкой спутников, АСУ химического завода или АЭС, полетами авиации, стратегическими вооружениями. Например, в марте 2001 г. появилась информация о том, что в Интернете были обнаружены украденные еще в декабре 2000 г. коды программы, применяемой в работе спутниковой навигационной системы "Навстар", используемой для обеспечения информацией военных и гражданских объектов по всему миру[16]. Попади эти данные в руки к террористам, последствия (типа террористических актов в США 11 сентября 2001 г.) могли бы стать катастрофическими. Начиная с середины 90-х годов XX в. систематические попытки осуществления "взлома" компьютерных систем ряда крупнейших компаний и государственных организаций с целью похищения коммерческих, технологических и иных секретов принимают угрожающие масштабы. По оценкам Комитета ООН по предупреждению преступности и борьбе с ней, компьютерная преступность вышла на уровень международных проблем[17].

Кроме того, информационные ресурсы используются террористическими группами для пропаганды своих целей, сбора денег, вербовки новых членов, координации преступных действий. Технические параметры ИЭС позволяют обеспечивать организационно-структурную целостность преступных организаций за счет предоставления возможности свободной связи и анонимности их участникам, а также оперативного решения вопросов финансирования преступных предприятий, скрывая источники происхождения денег, фактически в любой части земного шара.

Опытные хакеры все чаще становятся незаменимыми членами серьезных преступных организаций. С учетом всего этого следует отметить, что вхождение России в мировое информационно-электронное про-

[13] См.: *Николин Б.* Информационная война. Ближайшее будущее? // Инженер. 1996. № 9. С. 1–3, 27–31; *Его же.* Информационная война // Инженер. 1996. № 15. С. 9–25; *Черешкин Д.С., Смолян Г.Л.* Новости информационной войны // Конфидент. 1996. № 6. С. 19–21; *Завадский И.И.* Информационная война – что это такое? // Конфидент. 1997. Июль – август. С. 13–20; Росс. газ. 1997. 23 авг.

[14] *Лопатин В.Н.* Указ. соч. С. 240–241.

[15] Например, базы данных операций расчетно-кассовых центров Банка России и ряда других электронных баз в 2005 – 2006 гг., в том числе сведений о 45,7 млн. человек, использующих кредитные карты компании TJX в США.

[16] См.: Сегодня. 2001. 7 марта.

[17] См.: Сегодня. 2000. 14 апр.

странство предполагает самое пристальное внимание к вопросам безопасности личности, общества и государства.

Новая мера открытости мира, при которой человеку жить становится удобнее и комфортнее, таит в себе немало угроз. И то, что кажется странным, даже экзотическим и невозможным сегодня, через некоторое время за счет "размывания" норм нравственности, пропаганды насилия, жестокости и правового нигилизма может стать вполне приемлемым.

Так, со второй половины 90-х годов XX в. в США и Великобритании активно проводятся эксперименты по имплантации в тело людей микрочипов с полным объемом информации о них, не только исключающих необходимость в наличии паспортов и банковских карт, но и обеспечивающих возможность передачи таким субъектам определенных жизненных установок.

"Моделирование людей", создание тотальных форм социального контроля, рассмотрение человеческого мозга в качестве биохимической машины, которую требуется соответствующим образом "налаживать", проектируя поведение людей, разработка "оптимизированного человека", способного управлять не только своими страстями, интеллектом, поведением, но и продолжительностью жизни, – эти проекты получают все более серьезное внимание не только в научных лабораториях, но и в литературе, а также кинематографе. Сегодня есть все основания полагать, что XXI в. станет граничным на этапе фильтрации генов и попыток "улучшения породы" живых существ, в том числе коррекции генетического аппарата человека. С начала 90-х годов XX в. в рамках создания так называемых "интеллектуальных тканей", "живых компьютеров", "человеко-машинных гибридов" осуществляются эксперименты по сращиванию с организмом человека микропроцессорных систем для получения сверхмощного интеллекта и "гигантской" работоспособности. С середины 90-х годов также проводятся медицинские эксперименты по вживлению в мозг и тело человека микрочипов, обеспечивающих возможность его непосредственного подключения к глобальным базам компьютерных данных.

Следует отдавать себе отчет, что в начале третьего тысячелетия земная цивилизация оказалась в переломной точке своего исторического развития, переход через которую делает возможными различные варианты эволюции информационно-электронной среды. Защита – это всегда ограничение. В условиях нивелирования роли морали в современном обществе именно право призвано обеспечить безопасное развитие информационно-электронных систем. При этом необходимо дать четкий ответ на вопросы: что, как и для чего надо регулировать, во имя чего следует совершать принуждение над волей и поведением отдельных личностей и структур, устанавливать общепринятые правила отношений, вводить ограничения в жизнь социума и его членов[18]. Но для того, чтобы разумно построить систему правовых ограничений в современном обществе, важно понять, как правильно совместить использование доступа к электронным системам розыскной, ориентирующей, сигнальной, доказательственной, управленческой и другой информации и сохранить основы демократического развития общества.

Между тем в институтах власти на концептуальном уровне пока отсутствует понимание того, какая перспектива не столь отдаленного будущего может ожидать человека и общество. И это вопрос скорее правовой, а не философский. Именно в праве, которое несет в себе гуманистический и нравственный потенциалы, должны закрепляться ориентиры развития ИЭС, обеспечивающие безопасное существование человека, общества, государства. Применительно к развитию ИЭС в условиях усиления кибертерроризма великое изречение Протагора о том, что "человек есть мера всех вещей", дополненное Сократом – "только как мыслящий", приобретает новый смысл.

При этом регулятивная составляющая действия права предполагает выработку долгосрочных целей и стратегию их реализации. В качестве данных целей может рассматриваться достижение такого положения в обществе, при котором устраняются не только опасности для дальнейшего существования человека, общества, государства, но и причины, побуждающие личность совершать действия, приводящие к возникновению таких опасностей. В этой связи правовое регулирование безопасного развития информационно-электронных систем можно охарактеризовать как форму упорядочения общественных отношений, нацеленную на создание безопасных условий для человека, общества и государства в атмосфере усиления кибертерроризма.

Таким образом, правовое осмысление проектов, связанных с развитием ИЭС, должно быть ориентировано на обеспечение безопасного состояния человека, общества и государства. Действуя, право призвано "очерчивать" границы поведения людей в обществе, связывая их государственной и взаимной ответственностью. Человек как субъект действия права одновременно является и адресатом правовой регламентации, занимает центральное место (в рамках конкретной исторической эпохи) в системе указанных выше связей. При этом с точки зрения безопасности в концептуальном смысле следует особо выделить угрозу развития кибертерроризма. Для ее локализации целесообразно ввести понятие "информационная емкость права", под которым следует понимать разность между снятой и оставшейся неопределенностью у адресатов права после получения ими правовой информации. Данное понятие призвано характеризовать свойство правовых установлений, сохранять необходимые им качества в заданной форме, в том числе отражать логику построения правовых конструкций.

[18] *Бачило И.Л.* Глобальная информатизация и право // Проблемы информатизации. 1999. Вып. 3. С. 10–19.