УДК 342+347.77

И.Л. Сафронова

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ОСНОВНЫЕ ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

Отмечено, что угрозы информационной безопасности (возможное использование информационно-коммуникационных технологий в преступных, террористических и враждебных военно-политических целях; применение уязвимых аппаратных и программных продуктов в военном секторе) становятся важным фактором, непосредственно влияющим на формирование международных отношений, и приобретают особую остроту в связи со значительным отставанием международного права от стремительно развивающихся информационных отношений в обществе. Рассмотрены инициативы России по укреплению как международной информационной безопасности, в частности, в рамках ООН, так и информационной безопасности на национальном уровне.

За последнее время появилось значительное число публикаций по различным аспектам информационной безопасности. Действительно, данная проблематика приобретает всю большую актуальность. Связано это с несколькими обстоятельствами.

Стремительное развитие и использование информационно-коммуникационных технологий (ИКТ) имело решающее значение для перехода от индустриального к постиндустриальному, информационному обществу, открывающему широчайшие позитивные возможности для прогрессивного развития человека, общества, государства и международного сообщества в целом, распространения процессов демократизации, достижения устойчивого экономического роста.

Динамичное расширение информационного сектора повлекло за собой серьезные изменения в структуре мировой экономики. Так, в середине девяностых годов ИКТ, в первую очередь Интернет, стали повсеместно использоваться промышленными и торговыми предприятиями и организациями, банковско-финансовым сектором, транснациональными корпорациями. В формирующуюся глобальную электронную среду стали переноситься важнейшие составляющие торгово-экономической деятельности.

Индустрия информатизации и телекоммуникаций, информационных услуг на современном этапе развития человечества является одной из наиболее стремительно развивающихся сфер мировой экономики, способной конкурировать по доходности с топливно-энергетическим комплексом и автомобилестроением. Она сделала рынок значительно более масштабным, динамичным и конкурентным, дала стимул к зарождению множества новых видов бизнеса.

ИКТ по своей природе являются уникальным средством обработки, хранения и передачи информации с выходом на практически неограниченную аудиторию. Эта возможность позволяет правительствам предоставлять гражданам услуги в рамках программ электронного правительства (e-government); организациям – информировать о своей деятельности, внедрять в производственные процессы и процессы выполнения работ и оказания услуг безбумажные технологии (так называемые CALS-technologies), переходить на методы электронной коммерции; банковским и финансовым учреждениям – оказывать услуги управления банковским счетом через Интернет, осуществлять, задействовав информационные каналы, платежи в режиме реального времени; гражданам – участвовать в процессах принятия политических решений, эффективно искать и получать информацию, распространять результаты своего творческого труда, вступать в виртуальные сообщества в соответствии со своими интересами.

Сегодня правомерно утверждать: чем большими возможностями в информационной сфере обладает государство, тем с большей вероятностью при прочих равных условиях оно может добиться стратегических геополитических преимуществ и экономического процветания.

Вместе с тем глобальная информатизация может в ряде случаев прямо или опосредованно приводить к негативным последствиям: усугублению «цифрового разрыва» – неравенства в уровнях развития и внедрения ИКТ, а также доступа к ним как между разными государствами, так и внутри отдельных стран (именно такой – внутригосударственный – «цифровой разрыв» характерен для России на данном этапе), что может повлечь за собой дальнейшую поляризацию мира; размыванию понятия суверенитета государств; ослаблению национальной безопасности стран; нарушению основных прав и свобод человека в информационной сфере.

Высокая сложность и одновременно уязвимость всех систем, на которых базируются национальное, региональные и мировое информационные пространства, а также фундаментальная зависимость от их стабильного функционирования практически всех инфраструктур госу-

дарств как в гражданском, так и в оборонном секторе, в том числе критических, приводят к возникновению принципиально новых угроз. Особые опасения связаны с возможностью использования ИКТ в преступных, террористических и враждебных военно-политических целях против информационных ресурсов и инфраструктур.

Активизируется киберпреступность, которая в настоящее время рассматривается многими экспертами как стремительно нарастающая угроза безопасности и для отдельных государств, и для мирового сообщества в целом. Несмотря на усилия правоохранительных органов и спецслужб, направленные на борьбу с киберпреступностью и кибертерроризмом, число преступных актов с использованием ИКТ не уменьшается, а, напротив, постоянно увеличивается, возрастает их общественная опасность.

По данным Интерпола, Интернет стал той сферой, где преступность растет самыми быстрыми темпами. Каждый год в мире фиксируются сотни тысяч попыток несанкционированного вмешательства в государственные, военные, банковские, корпоративные компьютерные системы, компьютеры отдельных пользователей.

В настоящее время в мире насчитываются десятки тысяч различных вирусных программ и их модификаций, увеличивается количество взломов баз данных и сетевых ресурсов компаний, растут угрозы хищения конфиденциальной информации. По оценкам многих аналитиков, с 2001 г. характер взломов существенно изменился. Хакерство становится все более глобальным, масштабным по техническим (количество зараженных компьютеров), экономическим (замедление Интернет, сбои в работе сайтов, в частности электронной торговли, при осуществлении банковских и биржевых транзакций), а также возможным политическим последствиям (участившиеся проникновения в сети государственных министерств и ведомств, в том числе оборонных).

Ежегодные финансовые потери от незаконной деятельности с использованием новейших Интернет-технологий превышают 80 млрд долл. США.

Меняется облик терроризма, о чем наглядно свидетельствует появление информационного терроризма. ИКТ уже освоены международными террористическими и экстремистскими организациями (ХАМАС, Аль-Каида).

ИКТ предоставляют террористам возможность скрытно, планомерно и эффективно воздействовать на индивидуальное и массовое сознание, общественное мнение, процессы принятия решений; распространять информацию для вербовки в свои ряды новых членов, пропаганды собственных идей; осуществлять сбор денежных средств для финансирования своей деятельности; проводить дезинформацию; вызывать панику, а также непосредственно совершать террористические акты.

ИКТ позволяют террористическим группам, большинство из которых имеют в настоящее время сетевую организационную структуру, эффективно и скрытно осуществлять взаимодействие между ее разрозненными ячейками и отдельными членами, проводить сбор информации о будущих целях.

По оценкам экспертов, террористы уже сегодня способны использовать такие средства электронного воздействия, как, например, высокомощное микроволновое оружие, применение которого будет наиболее эффективным против критических информационных инфраструктур[1].

Что касается военного использования ИКТ, то такие прецеденты многочисленны: информационное оружие использовалось во всех военных конфликтах в течение последних 10-15 лет. Оно стало важной частью вооружения сил общего назначения США и их союзников. Имеются данные о том, что работы по развитию потенциала информационного противоборства проводятся более чем в 120 странах мира (разработки в области ядерного оружия ведут не более 20 стран[2]).

Происходит трансформация всей военной информационной архитектуры: наблюдается «информатизация» традиционных вооруженных сил и «интеллектуализация» вооружений. Активно развивается концепция сетецентрического ведения военных действий, подразумевающая достижение превосходства над врагом путем эффективной организации сбора, обработки и использования информации.

---

[1] *Sirak M.* U.S. vulnerable to EMP Attack // Jane's Defense Weekly. – 2004. – 26 July // http://www.janes.com/defence/news/jdw/jdw040726_1_n.shtml

[2] *Крутских А.В.* Война или мир: международные аспекты информационной безопасности / А.В.Крутских // Политика. – 2001. – № 45. – С. 11.

Сегодня можно говорить о том, что информационное оружие в некоторых развитых странах переходит в разряд тактического. Сообщается о разработках высотного электромагнитного импульсного оружия, способного выводить из строя электронику в радиусе сотен километров. Эксперты отмечают, что ряд стран такими возможностями располагают уже в настоящее время[3]. Ведутся разработки высокомощного микроволнового оружия, способного изменять траекторию ракет в полете, вызывать перегрузку или вывод из строя вражеских сетей связи, телеметрического оборудования и электроники, на которой в настоящее время основано все большее число систем вооружений[4]. Такое оружие будет способно поражать экранированное оборудование, защищенное от радиоактивного излучения[5], а также наносить ущерб здоровью лиц, находящихся в поле действия такого оружия, и даже причинять смерть[6].

Достижение превосходства в информационном противоборстве может предопределить исход военного противоборства в целом. Такое превосходство может достигаться без осуществления традиционных боевых операций, только за счет применения ИКТ.

Информационные операции зачастую ведутся в небоевой обстановке и проводятся за месяцы или даже годы до начала военной операции. Таким образом, военное по своей сути воздействие начинается без объявления войны, в мирное время. Информационные операции превращаются, таким образом, из вида боевых действий в самостоятельное мероприятие.

Применение инфооружия не обязательно вызовет разрушение объектов физической инфраструктуры и гибель людей. Жертва подчас может не осознавать, что находится под информационным воздействием. Тем не менее в результате таких действий происходит ослабление противника, и война может быть выиграна до ее начала. Можно прогнозировать, что в будущем доля информационного противоборства при проведении военных операций будет возрастать.

Использование информационного оружия не требует больших финансовых затрат, что делает информационную войну экономичным и потому весьма опасным средством вооруженной борьбы. Инфооружие не знает географических расстояний, оно подрывает традиционное понятие государственных границ, делая их технологически проницаемыми. Его применение носит обезличенный характер и позволяет замаскировать разрушительную по своим масштабам информационную операцию, проведенную государством, под киберпреступление, источник которого так и останется неизвестным, или акт кибертерроризма, реализованный международными террористами, не имеющими государственной принадлежности. Одновременно трудно определить государство, осуществившее информационную атаку, поскольку агрессия может реализовываться с территории третьих стран.

Информационное оружие стирает различия между военными целями и гражданскими объектами, что обусловлено значительной взаимосвязанностью и взаимозависимостью военных и гражданских информационных инфраструктур. Можно предположить, что в будущем высокотехнологичные гражданские информационные системы, в том числе поддерживающие работу критических гражданских инфрастуктур, станут все более частыми целями нападений со стороны возможных противников.

С другой стороны, тот факт, что в военном секторе многих стран используются коммерческие программные продукты, которые почти всегда имеют изъяны в защите, делает обороноспособность государств потенциально уязвимой для компьютерных нападений как хакеров и террористов, так и государств[7].

Проблему информационной безопасности в России обостряет фундаментальная зависимость российских информационных инфраструктур от зарубежных компьютерных средств. Почти 90% объемов продаж телекоммуникационного оборудования на внутреннем рынке (его емкость исчисляется миллиардами долларов) приходится на зарубежные оборудование, а также запасные части и комплектующие, используемые при его ремонте и обслуживании. Такая зависимость опасна не только с точки зрения экономической безопасности страны, но и безопасно-

---

[3] *Wilson C.* Information Operations and Computer Network Attack Capabilities of Today // International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law. Proceedings. Edited by K.Byström. – Stockholm: Swedish National Defence College, 2005. – P. 56.

[4] Там же. С. 50.

[5] *Abrams M.* The Dawn of the E-bomb // IEEE Spectrum Online. – 2003. – November // http://www.apectrum.ieee.org/WEBONLY/publicfeature/nov03/1103ebom.html

[6] *Matus V.* Dropping the E-Bomb // The Weekly Standard. 2003. – 2 February // http://theweeklystandard.com/Utilities/printer_preview.asp?idArticle=2209&R=9F0C225C3.

[7] *Murray B.* Navy carrier to run Win 2000. // GCN.com – 2000, 11 September // http://www.gcn.com/vol19_no27/dod/2868-1.html. См. также Lettice J. OSS Torpedoed: Royal Navy will run on Windows for Warships // The Register. – 2004. – 6 September // http://www.theregister.co.uk/2004/09/06/arms_goes_windows_for_warships

сти в более широком контексте, особенно с учетом того, что зарубежное программное обеспечение широко используется на стратегических объектах российского оборонного комплекса, и принимая во внимание реальные прецеденты закладки недокументированных функций в компьютерные микросхемы и интегрирования недокументированных программных модулей для осуществления вмешательства в работу программного обеспечения[8].

Эти негативные геополитические последствия информатизации представляют серьезную угрозу национальной и международной безопасности. Они стали важным фактором, непосредственно влияющим на формирование международных отношений, и приобретают особую остроту в связи со значительным отставанием международного права от стремительно развивающихся информационных отношений в обществе, недостаточностью существующих международно-правовых норм, регулирующих такие отношения, и многосторонних механизмов обеспечения международной информационной безопасности.

Опасный характер угроз информационной безопасности делает противодействие им принципиальным аспектом укрепления национальной, региональной и международной безопасности и стратегической стабильности, а вследствие этого – отдельным направлением внутри- и внешнеполитической деятельности всех государств, стремящихся интегрироваться в формирующееся глобальное информационное общество (ГИО), роль которого по мере развития будет, по-видимому, только возрастать.

Россия стала первым государством, на международном уровне поднявшим вопрос о появлении принципиально новых – информационных – угроз безопасности в XXI веке и необходимости укрепления международной информационной безопасности (МИБ) в целях эффективного обеспечения национальной и международной безопасности и стабильности, прежде всего за счет снижения угроз враждебного использования ИКТ.

Центральным форумом для продвижения российской инициативы по МИБ была избрана Организация Объединенных Наций. Постановка вопроса в Первом комитете Генассамблеи ООН (разоружение и вопросы международной безопасности) позволила сделать акцент прежде всего на военно-политической составляющей темы МИБ. В 1998 г. Россией впервые был внесен проект резолюции Генассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности».

На протяжении семи лет резолюции по МИБ, проекты которых предлагались Российской Федерацией, принимались на Генассамблее консенсусом. При этом их положения последовательно развивались и конкретизировались, в них закреплялись формулировки, отвечающие интересам безопасности стран мира и всего международного сообщества в целом. В резолюции были отражены все значимые моменты, в первую очередь признание «триады» угроз МИБ – военно-политического, террористического и криминального характера – и необходимости определения совместных путей и средств их минимизации.

В 2004-2005 гг. в рамках Группы правительственных экспертов ООН по МИБ (ГПЭ), созданной по инициативе России, было проведено исследование на экспертном уровне всего комплекса вопросов, связанных с информационной безопасностью. Группой были согласованы значительные по объему и содержательно важные разделы итогового доклада, однако выработать его полный текст, по которому мог бы быть достигнут консенсус, на том этапе не удалось. Причины этого очевидны. Проблематика МИБ носит комплексный характер и ставит перед международным сообществом принципиально новые и чувствительные вопросы, на которые необходимо сообща искать ответы. Ясно, что процесс этот не будет быстрым.

Принятие на юбилейной, 60-й, сессии ГА ООН очередной резолюции по МИБ (документ A/RES/60/45 от 8 декабря 2005 г.), ориентирующей международное сообщество на дальнейшее углубленное изучение угроз информационной безопасности и поиск, в том числе в формате ГПЭ, которая должна быть создана в 2009 г., многосторонних механизмов укрепления информационной безопасности на всех уровнях, ставит перед Россией и другими странами мира новые задачи. Для решения их, по мнению автора, принципиально важно исходить из следующего.

Существующие многосторонние механизмы, направленные на обеспечение информационной безопасности, недостаточны для эффективного решения вопросов международной информационной безопасности, адекватного угрозам в этой сфере. Подход, предусматривающий многоаспектное и всестороннее обеспечение информационной безопасности на национальном, ре-

---

[8] *Акимов Ф.* Кто владеет информацией (интервью с членом комитета Госдумы по безопасности, генерал-лейтенантом налоговой полиции В.Волковским) // http://www.lgz.ru/archives/html_arch/lg102002/Polosy/art4_1.htm

гиональном и глобальном уровнях в привязке к триаде угроз военно-политического, криминального и террористического характера, предусматривается только российской инициативой по МИБ.

Вопросы регулирования сферы информационного противоборства в полной мере не подпадают под действие ни одного из существующих на сегодняшний день международных политико-правовых документов. Документы, так или иначе затрагивающие проблематику международной информационной безопасности, оказываются либо недопустимо суженными по своему предмету и/или географическому охвату, либо допускают множественность трактовок основных понятий. Соответствующие национальные законодательства являются недостаточными в силу своей разнородности и недостаточно высокой степени гармонизации, а также по причине трансграничности ИКТ.

Эффективное противодействие угрозам в информационной сфере возможно за счет кодификации и прогрессивного развития соответствующих норм международного права для обеспечения эффективного регулирования отношений, возникающих в информационном пространстве, на базе продолжения консультативного и переговорного процессов на двустороннем, региональном и международном уровнях, в том числе путем выработки и принятия нового политико-правового документа, такого как принципы деятельности или кодекс поведения государств в области международной информационной безопасности, многостороннего договора о борьбе с информационным терроризмом, а в перспективе – юридически обязательного международного договора, регулирующего отношения в области международной информационной безопасности.

При этом, предпринимая необходимые усилия на международном уровне в направлении снижения угроз информационной безопасности, которые имеют внешний характер и могут исходить как от преступников, террористов, так и от отдельных государств, крайне важно вести работу внутри страны по укреплению инфобезопасности на национальном уровне.

Необходимо последовательно вести дело к ликвидации внутрироссийского «цифрового разрыва», ослабляющего информационную и – в целом – национальную безопасность России: активно развивать отечественную информационно-телекоммуникационную инфраструктуру, расширять доступ российских пользователей к информационным технологиям, средствам и ресурсам, а в конечном итоге – к информации; развивать возможности, предоставляемые в рамках программы электронного правительства.

Принципиальное значение имеет поддержка разработок и производства в России конкурентных инфокоммуникационных средств на отечественной микроэлектронной базе; применение таких средств в России, прежде всего в оборонном комплексе и на объектах критической гражданской инфраструктуры; экспорт таких изделий; разработка и производство программного обеспечения в интересах как российских, так и зарубежных пользователей.

По мнению автора, существующая нормативно-правовая и организационная база для реализации этих мероприятий в целом не носит целостного, системного характера и нуждается в укреплении. Требуется выработка и проведение комплексной промышленной политики в России, которая бы увязывала действующие федеральные целевые программы, налоговую и таможенную политику.

Только таким образом, как представляется, можно укрепить информационную безопасность Российской Федерации, содействовать обеспечению международной информационной безопасности, отвечающей интересам безопасности на национальном, региональном и международном уровнях, рассчитывать на равноправное и недискриминационное включение в глобальное информационное общество и максимальное использование предоставляемых им преимуществ.