УДК 341:004.056

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

© 2015 А.В. Балановская*

Ключевые слова: международная информационная безопасность, угрозы, киберпреступления, информационно-коммуникационные технологии, государственная политика.

Проанализирован достигнутый уровень обеспечения информационной безопасности в международном аспекте, представлена позиция Российской Федерации относительно проблем международной информационной безопасности, а также направления их решения.

В эпоху становления и развития глобальной информационной экономики противодействие различным угрозам и вызовам, рожденным этой эпохой, становится серьезной проблемой, которая затрагивает вопросы обеспечения всестороннего устойчивого функционирования и развития как современного мира, так и отдельно взятых объектов в текущей и стратегических перспективах. Эффективное решение этой проблемы возможно при совместном объединении усилий всего международного сообщества. Сдерживание и предотвращение существующих и возможных угроз в информационной сфере сегодня считается наиболее серьезным вызовом безопасности национальным и международным экономикам.

В процессе обеспечения международной информационной безопасности серьезная озабоченность исследователей возникает в связи с развитием информационно-коммуникационных технологий, которые получили в современном мире беспрецедентное развитие. В особенности хочется выделить развитие возможностей применения глобальных сетей в целях, которые, по меньшей мере, не совместимы с задачами по обеспечению стабильности и международной безопасности.

Обособленно стоит проблема информационных угроз при использования различными информационными сетями. В современных условиях сеть как система децентрализованного управления приобретает все большее значение. По сетевому принципу фирмы строят свои внутренние и внешние связи[1].

Неправомерный доступ злоумышленника к информационным ресурсам приводит к блокировке, копированию, сбоям в работе сетей, нарушает деятельность систем, организованных для осуществления автоматизированного контроля и управления в различных объектах как промышленности, так и жизнеобеспечения, обороны, транспорта, и в конечном счете может привести не только к материальному ущербу, но и к причинению вреда здоровью людей, а в худшем случае даже к их гибели.

Применение информационно-коммуникационных технологий в деструктивных целях позволяет обеспечить их общедоступность, часто избирательность, а в случае необходимости и неизбирательность воздействия, сохранить анонимность применения, маскировку под конструктивную деятельность, минимизировать затраты при высоком уровне эффективности, а также расширить область применения до уровня трансграничного.

В процессе выработки позиции по проблеме обеспечения международной информационной безопасности в Российской Федерации аналитики исходили из наличия группы взаимосвязанных видов угроз военно-политического, криминального и террористического характера. Кроме того, применение информационно-коммуникационных технологий возможно не только отдельными злоумышленниками, криминальными группами, террористическими и экстремистскими организациями, но и целыми государствами в различных враждебных политических, во-

* Балановская Анна Вячеславовна, кандидат экономических наук, доцент Самарского государственного экономического университета. E-mail: balanovskay@mail.ru.

енных и экономических целях. Подобная деятельность позволяет осуществить агрессию скрытым образом и создать серьезные угрозы для безопасности на национальном уровне. В связи с таким видением данной проблемы Россией в настоящее время действуют "Основы государственной политики РФ в области международной информационной безопасности на период до 2020 года". Данный документ разрабатывался Советом безопасности, но в работе над ним приняли участие Министерство иностранных дел, Министерство связи и массовых коммуникаций, Министерство юстиции, Министерство обороны.

В документе сведены в единое целое ключевые инициативы в сфере международной информационной безопасности. По замыслу его разработчиков такой подход будет способствовать их продвижению на международном уровне и улучшению межведомственного взаимодействия внутри самой России.

В некоторых источниках говорится, что разработка и принятие данного документа могут расцениваться как симметричный ответ на принятую в 2011 г. США "Международную стратегию по действиям в киберпространстве". Предшественницей данного документа была "Национальная стратегия по обеспечению безопасности киберпространства" 2002 г. При разработке документов ставилась цель создания системы адекватного реагирования на возможные атаки, направленные на национальные информационные системы и сети, которые во многом являлись фундаментом инфраструктуры и от которых во многом зависит благополучие страны. В новом документе США "впервые приравняли акты компьютерных диверсий к традиционным военным действиям, оставив за собой право реагировать на них всеми средствами вплоть до применения ядерного оружия"[2].

Однако утверждение, что "Основы государственной политики РФ в области международной информационной безопасности на период до 2020 года" разрабатывались в связи с деятельностью других стран, весьма спорное. Так, в феврале 2011 г. Германия приняла документ под названием "Стратегия безопасности в киберпространстве", а также основала Национальное агентство киберзащиты. Данное агентство по своему функционалу тесно взаимодействует с полицией, разведкой и Федеральным управлением по информационной безопасности.

Германская стратегия, как и американская, включает секретную часть. Предположительно, засекреченная часть посвящена предлагаемым контрмерам, направленным на противодействие информационным атакам.

Схожий документ действует и в Великобритании также с 2011 г.

В мае 2013 г. в Индии принята стратегия в области кибербезопасности. Стратегия предполагает усиление защиты путем создания сети правительственных агентств, финансирование которых будет направлено на развитие исследований в области кибербезопасности.

В Евросоюзе стратегия кибербезопасности вступила в силу 19 июня 2013 г. На следующие семь лет, согласно документу, продлены полномочия и права Европейского агентства сетей и информационной безопасности. Правительствам стран Евросоюза в обязательном порядке предписано создать органы, которые бы отвечали за кибербезопасность, а крупным финансово-промышленным группам и компаниям - разработать меры по противодействию киберугрозам.

В стратегиях США и Индии разработчики в качестве основы действия заложили повсеместное сотрудничество между частным и государственным секторами.

Можно заметить, что российский вариант стратегии обеспечения кибербезопасности предполагает более мягкий сценарий развития, заключающийся в намерении бороться с возможными угрозами не методами военного реагирования, а путем укрепления международного сотрудничества.

В основах государственной политики РФ в области международной информационной безопасности на период до 2020 г. выделены "четыре основные угрозы в сфере международной информационной безопасности. Первая - использование информационно-коммуникационных технологий в качестве информационного оружия в военно-политических целях, для осуществления враждебных действий и актов агрессии. Вторая - применение

информационно-коммуникационных технологий в террористических целях. Третья - киберпреступления, включая неправомерный доступ к компьютерной информации, создание и распространение вредоносных программ"[3].

Эти три угрозы являются исторически общепризнанными и зафиксированы в различных документах Организации Объединенных Наций. Четвертая угроза, указанная в документе, отражает российский подход к проблеме. Эта угроза касается использования интернет-технологий для "разжигания вражды", "нарушения общественного порядка", "вмешательства во внутренние дела государств" и "пропаганды идей, подстрекающих к насилию". На эту угрозу исследователи обратили внимание после событий, произошедших в ряде стран, которые наглядно продемонстрировали все возможности Интернета, и в первую очередь социальных сетей, которые повсеместно были использованы для организации, управления и координации акций, направленных на расшатывание общеполитической обстановки и разжигание насильственных действий.

В борьбе с этими угрозами Россия будет опираться и на совместную работу со своими союзниками, такими как страны - члены Шанхайской организации сотрудничества, страны Организации договора коллективной безопасности, а также страны БРИКС. Совместная работа позволит добиться реализации широкого круга инициатив по решению данной проблемы на международном уровне, к которым относятся выработка общепризнанных правил поведения в киберпространстве, установление правового режима нераспространения информационного оружия, интернационализации систем управления Интернетом и т.д.

Россия предлагает сотрудничество путем диалога при условии наличия даже минимальных доверительных отношений. Относительно недавно президенты Российской Федерации и Соединенных Штатов Америки заключили соглашение, направленное на недопущение перерастания кибердиверсий в международные конфликты. Подобная практика предлагается также и для других стран.

В качестве приоритетной при рассмотрении общего контекста проблемы международной информационной безопасности в России рассматривается военно-политическая составляющая. При этом информационная кибервойна определяется как "противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба критически важным информационным системам, процессам и ресурсам, другим структурам подрыва политической, экономической и социальной систем, массированной и психологической обработки населения для дестабилизации общества и государства"[4]. Российская Федерация исторически первая обратила внимание всего международного сообщества на данные вызовы современности и те проблемы, которые придется решать в теперешних условиях.

При активном участии России в настоящее время создаются группы правительственных экспертов различных стран с целью проанализировать и выявить реальные и возможные угрозы в сфере международной информационной безопасности, разработать единые направления международного сотрудничества по противодействию выявленным угрозам, меры снижения потенциальных рисков, ликвидировать существующие информационные уязвимости.

Ежегодно проводится большое количество мероприятий, двусторонних консультаций по проблемам международной информационной безопасности, а также осуществляется практическая работа в данном направлении.

Цель усилий России по обеспечению международной информационной безопасности - "снижение угрозы нарушения мировой стабильности и безопасности международного сообщества в информационном пространстве на основе недопущения очередного витка гонки вооружений на качественно новом уровне развития информационно-коммуникационных технологий, защиты информационных ресурсов и критической информационной инфраструктуры в интересах развития общества, ограничение агрессивного использования информационно-коммуникационных технологий в целях силового решения межгосударственных противоречий"[5].

Результаты международных обсуждений данной проблемы, проводимых при участии правительств европейских стран, подтвердили, что возможные нападения на информационные сети в периоды вооруженных конфликтов и практическое применение информационно-коммуникационных технологий у специалистов не вызывает сомнения. Отметим, что возможный результат применения в масштабе страны информационного оружия можно сравнить с применением оружия массового поражения. Такие оценки подкрепляются практикой создания в рамках вооруженных сил отдельных государств специализированных подразделений для ведения военных действий на глобальном информационном пространстве.

В настоящее время во многих странах отмечается активизация преступлений с использованием информационных ресурсов и технологий. При этом данная категория преступлений фактически не имеет границ и открывает огромные возможности на глобальном уровне. Киберпреступность расширяет свое воздействие на новые сферы деятельности и является самой серьезной угрозой международной безопасности, реально приобретая характер транснациональной организованной преступности. Борьба с этой преступностью усложняется отсутствием международных соглашений, предусматривающих меры борьбы с компьютерными преступлениями.

Сегодня перед мировым сообществом стоит актуальная задача разработки, согласования и утверждения требований, положений, регламентов для противодействия киберпреступности. Рассматривая процесс реализации угроз, приходим к пониманию сущности угроз и выбора правильной стратегии по противодействию им[6].

Можно предложить ряд основных направлений для совместной работы, которые будут способствовать движению международного сообщества к созданию системы международной безопасности.

К ним можно отнести:

♦ развитие действующих норм международного права в области безопасности в направлении разработки эффективной системы превентивных действий для возможных агрессивных атак с применением информационно-коммуникационных технологий. Новые разработки будут содействовать развитию накопленного опыта и его применению для устранения возможных угроз;

♦ усиление международного сотрудничества в вопросах укрепления безопасности функционирования информационных сетей, относящихся к открытому типу, таких, как Интернет. Целесообразно разработать и обеспечить выполнение правовых механизмов, которые смогли бы повысить доверие к данным ресурсам. Этого можно достигнуть путем интернационализации управления такими сетями. Следует гарантировать расследование и уголовное преследование юридических и физических лиц, причастных к киберпреступлениям, даже если деяние совершено в рамках юрисдикции одной страны при негативных последствиях для других стран;

♦ международное сотрудничество в вопросах стандартизации требований по проблемам обеспечения информационной безопасности информационно-телекоммуникационных систем и информационных ресурсов. Подобные стандарты сформируют единый подход и позволят согласовать механизмы защиты в рамках информационных систем как национального, так и глобального уровня. Этот аспект особенно важен при создании и использовании глобальных компьютерных сетей, при осуществлении межгосударственного информационного обмена, а также в случае предоставления гражданам услуг, связанных с глобальным информационным пространством;

♦ большой вклад в решение проблемы может внести и научное сообщество. Приведение существующих наработок и международных подходов к единому пониманию позволит в диалоговом режиме разговаривать на одном языке, обеспечивая при этом максимальный эффект от произведенных усилий.

В заключение следует заметить, что за достаточно короткий период уже удалось выработать основополагающие подходы к представлению источников угроз международной информационной безопасности. На ближайшую перспективу необходимо поставить в качестве цели определение системы первоочередных мер по эффективному противодей-

ствию данным угрозам. Безусловно, не завершен сложный процесс системного осмысления международных проблем развития безопасного глобального информационного общества. Очень важно сохранить достигнутую позитивную динамику, наращивать объемы взаимоотношений и обеспечивать взаимопонимание, быть готовыми к нахождению различного рода компромиссов и далее развивать практическое взаимодействие по различным направлениям международного сотрудничества.

---

[1] *Казарин С.В., Ашмарина С.И.* Информационное общество как современная среда осуществления социально-экономических процессов // Вестник Самарского государственного экономического университета. 2012. № 11 (97). С. 49.

[2] *Хорунжий Н.* Нужно ли России киберкомандование? // Военное обозрение. 2013. URL: http://topwar.ru/32230-nuzhno-li-rossii-kiberkomandovanie.html.

[3] *Черненко Е.* Мир домену твоему. Россия определилась с политикой информационной безопасности // Коммерсантъ. 2013. URL: http://www.kommersant.ru/doc/2245463.

[4] *Шерстюк В.П.* Угроза международной информационной безопасности в условиях формирования глобального информационного общества и направления сотрудничества // Право и безопасность. 2011. № 4 (37). С. 62.

[5] Там же. С. 60.

[6] *Балановская А.В.* Модель угроз информационной безопасности // Вестник Самарского государственного экономического университета. 2011. № 9 (83). С. 20.

Поступила в редакцию 13.04.2015 г.