ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕГИОНАЛЬНОМ СОДРУЖЕСТВЕ В ОБЛАСТИ СВЯЗИ

ГЕНЕРАЛЬНЫЙ ДИРЕКТОР ИСПОЛНИТЕЛЬНОГО КОМИТЕТА
РЕГИОНАЛЬНОГО СОДРУЖЕСТВА В ОБЛАСТИ СВЯЗИ
Нурудин Насретдинович Мухитдинов

Информационно-коммуникационные технологии с каждым днем все прочнее входят в нашу жизнь: используются в быту, на работе, в обучении, в медицине, в торговле, облегчают взаимодействие с государственными органами и т.д. Мы живем в эпоху «виртуальной реальности».

Однако существующие в реальной действительности негативные элементы, такие как мошенничество, преступность, проявления насилия, неотвратимо проецируются в «виртуальный мир» – спам, вирусы, хакерство, распространение детской порнографии, киберпреступность, кибертерроризм и др. Киберпространство не имеет пределов и границ, киберугрозы могут возникнуть где угодно и нанести огромный ущерб за считаные минуты. Поэтому повышение доверия и безопасности при использовании информационно-коммуникационных технологий (ИКТ) является одной из самых актуальных проблем для мирового сообщества.

Впервые проблема обеспечения информационной безопасности в глобальном масштабе была обозначена в «Окинавской хартии глобального информационного общества», принятой в 2002 году лидерами стран G8 («Большой восьмерки»). Следующим этапом стала Всемирная встреча на высшем уровне по вопросам информационного общества (ВВУИО). Для стран СНГ важное значение имеет встреча на высшем уровне «Соединим СНГ». В итоговых документах саммитов отражена необходимость принятия реальных мер по обеспечению безопасности при использовании ИКТ на глобальном, региональном и национальном уровнях.

Реализация решений ВВУИО в части обеспечения информационной безопасности осуществляется в рамках направления деятельности ВВУИО «Укрепление доверия и безопасности при использовании ИКТ». В этом процессе активная роль отводится Международному союзу электросвязи (МСЭ). Направления деятельности МСЭ в данной сфере определены соответствующими резолюциями ООН, актами и решениями полномочных конференций МСЭ 2010 года, Хайдарабадским

планом действий по развитию электросвязи, Глобальной программой кибербезопасности, начатой по инициативе генерального секретаря МСЭ Х. Туре, а также другими документами МСЭ. Вопросы укрепления доверия и безопасности, управления определением идентичности, защиты детей от онлайновой эксплуатации, неприкосновенности частной жизни и защиты данных, кибербезопасность и т.д. были отражены в отчете генерального секретаря МСЭ и активно обсуждались на Всемирном форуме по политике электросвязи МСЭ.

Региональное содружество в области связи (РСС) было образовано в 1991 году министрами связи вновь созданных независимых государств на постсоветском пространстве с целью сохранения и гармоничного развития сетей почтовой и электрической связи. РСС является открытой международной региональной организацией в области связи, в состав которой наряду с полноправными членами – странами СНГ – входят наблюдатели – администрации министерств связи Болгарии, Латвии, Словении, операторы связи Эстонской Республики и Международная организация космической связи «Интерспутник».

Признавая масштабность преобразований в сфере ИКТ, страны Содружества в 2002 году по решению Совета глав правительств СНГ создали при РСС Координационный совет государств – участников СНГ по информатизации (Координационный совет). Его членами являются национальные органы по информатизации из девяти стран Содружества.

Одним из важнейших достижений Координационного совета стала разработка и утверждение Советом глав правительств СНГ в ноябре 2006 года решения «О стратегии сотрудничества государств – участников СНГ в сфере информатизации и плане действий по реализации Стратегии сотрудничества государств – участников СНГ в сфере информатизации на период до 2010 года».

В части обеспечения информационной безопасности стратегия предусматривала: проведение анализа существующих и потенциальных угроз, решение вопросов защиты государственных информационных систем от несанкционированного доступа и обеспечения их безопасного взаимодействия на национальном и межгосударственном уровне, защиты баз данных, персональных данных, борьбы с киберпреступлениями, оперативного реагирования на случаи нарушения информационной безопасности и др.

Стратегические задачи РСС в вопросах обеспечения информационной безопасности четко отражены в проекте стратегии сотрудничества государств – участников СНГ в построении и развитии информационного общества и плане действий по ее реализации на период до 2015 года, в разделе «Информационная безопасность».

Для расширения взаимодействия по вопросам обеспечения информационной безопасности и выработки общих подходов к их решению в конце 2004 года при Координационном совете была создана Комиссия по информационной безопасности.

В декабре 2011 года в целях расширения состава участников решением Совета глав АС РСС Комиссия была преобразована в Комиссию РСС по информационной безопасности (далее – Комиссия). Учитывая специфику тематики, в состав Комиссии наряду с представителями администраций связи РСС входят работники компетентных органов в данной сфере из стран Содружества.

Также в целях привлечения научных кругов к деятельности Координационного совета и Комиссии была определена головная организация по научному обеспечению вопросов информационной безопасности – ФГУП ВНИИПВТИ (Российская Федерация). При Комиссии действует общественный консультативный совет по научно-технологическим вопросам информационной безопасности, который оказывает помощь в подготовке и экспертизе документов, организации семинаров и др.

Вопросу обеспечения защиты информации и безопасности информационных ресурсов уделяется большое внимание на самом высоком уровне. Признавая, что актуальность и обеспечение технологической независимости и информационной безопасности государства является стратегической задачей, главы государств СНГ в октябре 2008 года утвердили Концепцию сотрудничества государств – участников СНГ в сфере обеспечения информационной безопасности и Комплексный план мероприятий по ее реализации. Принятие этих документов способствовало дальнейшему формированию и совершенствованию правовой основы межгосударственного сотрудничества в данной сфере и созданию защищенной информационной среды на пространстве СНГ.

При этом хотелось бы отметить, что Координационный совет определен основным исполнителем мероприятий Комплексного плана.

В целях реализации ряда мероприятий, предусмотренных Комплексным планом, в рамках РСС была организована и проведена научно-исследовательская работа. В ходе НИР проанализировано текущее состояние, проблемы и первоочередные задачи обеспечения информационной безопасности в СНГ, включая анализ законодательств государств – участников СНГ, регламентирующих обеспечение информационной безопасности. Подготовленный анализ использован при подготовке аналитического доклада Совету глав правительств СНГ.

Комиссией по информационной безопасности подготовлены проекты Соглашения о сотрудничестве государств – участников СНГ в области обеспечения информационной безопасности и Положения о базовой организации государств – участников СНГ, осуществляющей методологическое и организационно-техническое обеспечение работ в области информационной безопасности и подготовку специалистов в этой сфере.

Сегодня «Положение о базовой организации государств – участников СНГ, осуществляющей методологическое и организационно-техническое обеспечение работ в области информационной безопасности и подготовку специалистов в этой сфере», а также кандидатура ФГУП ВНИИПВТИ в качестве базовой организации в области информационной безопасности утверждены Советом глав правительств СНГ. Членами Комиссии совместно с ФГУП ВНИИПВТИ готовятся:

- проект Соглашения о порядке признания юридической значимости электронных документов в международном информационном обмене между государствами – участниками СНГ на базе основных принципов, изложенных в Модели ПД-Т;
- предложения по осуществлению трансграничного информационного обмена, связанного с контролем над импортом и экспортом ИКТ-продуктов, содержащих криптографические функции и средства защиты информации в государствах – участниках СНГ.

Очень своевременен прорабатываемый в рамках РСС вопрос о создании Единого центра по обеспечению безопасности в киберпространстве государств – участников РСС (Единый центр РСС). Единый центр РСС призван стать аналитическим, координационным центром для пользователей информационных систем и сети Интернет в вопросах обеспечения информационной безопасности и защиты информационных ресурсов государств – участников РСС.

В соответствии с появлением возможности использования широкополосного доступа к сети Интернет существенно увеличилось количество пользователей. Часть этих пользователей – дети, для которых существует множество угроз и рисков, связанных с использованием сети Интернет, отсюда и возможные негативные последствия. Кроме того, дети являются наиболее уязвимыми пользователями сети Интернет.

Большую роль в борьбе с негативными проявлениями сети Интернет в отношении несовершеннолетних играют международные организации, а также национальные и государственные структуры. Как пример в России было создано общественное объединение «Лига безопасного Интернета», куда вошли представители общественных организаций, независимого гражданского общества, крупнейших операторов связи, контент-провайдеров, правоохранительных органов, Федерального Собрания, с тем чтобы не только начать обсуждать эти проблемы, но и предпринимать конкретные меры именно по линии гражданского общества.

Только за год деятельности лиги в России было закрыто порядка 10 тыс. ресурсов, которые содержали материалы, противоречащие нравственности, 1,5 тыс. материалов, содержавших элементы наркопропаганды. Борьба ведется не только в сети, но и за ее пределами. В частности, с помощью этих общественных организаций и сигналов, которые поступали от граждан, была разоблачена крупнейшая педофильская сеть в России – свыше 130 человек. Ее организаторы уже арестованы, привлекаются к ответственности.

Обсуждаются меры, которые еще могли бы быть предприняты. В частности, называются такие приемы, как введение так называемых белых и черных списков.

Белые списки иначе известны как детский Интернет – это набор программ, ресурсов, которые прошли аккредитацию и сертификацию, получили одобрение родительских ассоциаций, ассоциа-

ций педагогов, психологов и безвредны для детей. Также необходимо введение так называемых черных списков – это как раз те ресурсы, которые противоречат законодательству, нормам нравственности.

Безопасность детей в Интернете приобретает особую значимость с началом нового учебного года. Новая услуга «Детский Интернет», расширяет список сервисов «МегаФон», которые обеспечивают безопасность детям и спокойствие родителям. Услуга «Детский Интернет» оградит ребенка от посещения сайтов, содержащих «взрослый» контент, нецензурную лексику или призывы к насилию. Просматривать можно будет интернет-страницы из белого списка, который содержит более 800 тыс. проверенных русскоязычных сайтов. При попытке открыть нежелательный сайт пользователь автоматически перейдет на страницу deti.megafon.ru/forbidden, где можно найти детскую коллекцию сайтов, пожаловаться на сайт, а также отправить заблокированный сайт на проверку, если родители, считают, что данный ресурс должен быть доступен для ребенка.

В Украине компания «Киевстар» проводит системную работу в развитии интернет-технологий, повышении безопасности детей в Интернете, их грамотности и этики поведения в сети. Для абонентов компании «Киевстар» разработана также бесплатная услуга «Родительский контроль», обеспечивающая посещение ребенком с мобильного телефона гарантированно безопасных сайтов.

Подобная системная работа в области обеспечения безопасности детей в Интернете проводится РУП «Белтелеком» и рядом других операторов электросвязи РСС.

В 2010 году ведущие российские интернет-провайдеры подписали Хартию операторов связи России по борьбе с детской порнографией в сети Интернет. Подписание хартии стало естественным продолжением усилий ведущих российских интернет-провайдеров в области защиты от противоправной информации и детской порнографии в информационно-коммуникационных системах. Хартия закрепляет намерение операторов содействовать увеличению безопасности при работе в Интернете и совместно бороться с производством, хранением, предоставлением и распространением детской порнографии в сети. В рамках хартии операторы взяли на себя обязательство осуществлять защиту пользователей сети Интернет от контакта с детской порнографией всеми законными способами, включая пресечение производства и хранения детской порнографии и блокировку доступа к подобным ресурсам. Кроме того, операторы обязуются предоставить пользователям техническую возможность самостоятельно защитить себя от детской порнографии и другой противоправной информации.

Вопрос возможности присоединения к Хартии операторов электросвязи РСС рассматривался на заседании Координационного совета.

Относительно правового поля в области ИКТ важное значение по формированию и осуществлению согласованной законодательной деятельности, укреплению интеграционного взаимодействия на основе сближения национальных законодательств стран Содружества в области связи и информатизации имеет подписанное в декабре 2002 года «Соглашение о взаимодействии между Региональным содружеством в области связи и Советом Межпарламентской Ассамблеи государств – участников СНГ». С этой целью в 2003 году был создан и действует Экспертный совет МПА СНГ – РСС. За период деятельности Экспертного совета по предложениям участников РСС разработаны и приняты более 19 модельных законов. Разрабатываемые МПА СНГ модельные законы становятся реальной базой, которую парламенты стран СНГ могут использовать в своих странах при изменении и совершенствовании национального законодательства. Так по предложениям и при экспертной поддержке участников МПА СНГ – РСС был подготовлен и 16 мая 2011 года принят модельный закон «Об основах регулирования Интернета» (в России в июле 2012 году был принят закон о защите детей в сети Интернет).

Отрабатываются концептуальные подходы к разработке проекта Рекомендаций по совершенствованию и гармонизации национального законодательства государств – участников СНГ в сфере обеспечения информационной безопасности.

В заключение хотелось бы отметить, что сотрудничество государств – участников СНГ в сфере обеспечения информационной безопасности по обеспечению неприкосновенности и сохранности персональных данных граждан, совместной защите интересов в информационной сфере во многом способствует построению открытого, направленного на активное развитие информационного общества.