и развитию». Он развеял опасения и домыслы, сопровождающие разработку и принятие этого акта (вводится политическая и иная цензура в Интернете и российских СМИ; закон не применим к отношениям, осуществляемым с применением интернет-технологий, поскольку содержит невыполнимые требования, провоцирует неоднозначное толкование).

Однако конструктивная критика была услышана участниками обсуждения. Было отмечено, что следует серьезно заняться продвижением закона: решать вопросы финансирования деятельности всех причастных к исполнению предписанных норм; быстрее устранить неопределенность статуса «уполномоченного органа» по защите детей от «вредной информации» и недостаточность учета возможностей саморегулирования (самоорганизации) в сфере защиты детей от «вредной информации».

Участники Форума сошлись во мнении, что блокирование определенных сайтов может положительно сказаться на общем снижении потребления нелегального контента в Интернете, но лишь в том случае, если оно является составляющей частью более общих мер по борьбе с нелегальным контентом.

Ни один из существующих технических способов блокировки не может быть абсолютно эффективным – у каждого из них есть недостатки, которые сказываются на общей производительности Сети и несут угрозу свободе слова и правам пользователей. Любой из способов блокировки может быть обойден опытным пользователем с минимальными навыками.

Ни одна система возрастной маркировки или контентной фильтрации не способна заменить родительский контроль; она не подтвердила свою эффективность.

В целях повышения эффективности мер необходимо сочетание всех методов предотвращения появления и распространения в Интернете противоправного контента – законодательных, технических, мер саморегулирования и образования пользователей. Помимо этого необходимы срочные поправки в ФЗ № 436 «О защите детей от информации, причиняющей вред их здоровью и развитию».

Нужно установить обязательность наличия у каждого интернет-ресурса пользовательских соглашений для определения границ использования интернет-технологий при распространении информации третьих лиц (user-generated).

На Форуме активно обсуждался опыт общественных организаций. Участники «круглого стола» «Вопросы создания позитивного контента для детей» познакомились с практикой портала Блог школьного Всезнайки www.e-parta.ru, о котором рассказал его руководитель *Сергей Абрамов*. Начав с причин интереса подростков к вредной информации (синдром интеллектуальной пассивности, особенности физиологического развития, отсутствие опыта и навыков жизни во взрослом мире и нехватка позитивного контента), он рассказал, как можно решить эту проблему. Для этого необходима государственная политика, направленная на повышение медиаграмотности населения посредством включения специальных курсов в образовательную сферу.

На Форуме работала выставка «Безопасный Рунет 2012», на которой компании представили продукты обеспечения пользовательской безопасности. В частности, большое внимание привлекла уникальная доменная зона («.дети»), которая поможет детскому Интернету в России. Специальный стенд информировал, по каким принципам будет управляться это специальное интернет-пространство, как детский Интернет сделать не только безопасным, но и увлекательным и полезным для детского образования и развития.

Абакар АМИРХАНОВ

РЕЗОЛЮЦИЯ 14-ГО НАЦИОНАЛЬНОГО ФОРУМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В ходе работы 14-го Национального форума информационной безопасности (Инфофорум-2012) был рассмотрен широкий спектр проблем стратегического, организационно-правового, технологического и гуманитарного характера, в том числе:

- новые вызовы и угрозы в информационном обществе и формирование стратегии международной и национальной информационной безопасности;
- развитие электронных услуг населению;
- проблемы трансграничного электронного взаимодействия;
- проблемы развития национальной программной платформы и решения для обеспечения информационной безопасности;
- обеспечение информационной безопасности при создании информационно-аналитических систем нового поколения в органах государственной власти;
- инновационные решения для безопасности жизнедеятельности населения городов и регионов:
- проблемы обеспечения информационной безопасности при развитии «облачных» и грид-технологий;
- проблемы подготовки специалистов в сфере информационной безопасности и оценки потребности рынка.

Участники обсуждения констатируют следующее.

Становление глобального информационного общества, в частности в России, носит необратимый характер. Однако все развитые страны и международные организации обеспокоены тем, что

В №1 за 2012 г.

«Инфофорум – 2012» – обзор мероприятий состоявшегося в Москве 7-8 февраля 14-го национального форума «Информационная безопасность России в условиях глобального информационного общества».

широкое применение информационных технологий нанесет ущерб правам человека, общественной нравственности и безопасности государств.

Совет Европы, НАТО, США, Великобритания, Канада и ряд других государств приняли свои стратегии кибербезопасности. В России же принятая более 10 лет назад Доктрина информационной безопасности не получила адекватного стратегического развития. Целостная система комплексного противодействия использованию потенциала информационных технологий в целях угрозы национальным интересам России не создана.

В рамках долговременной стратегии развития информационного общества реализуется масштабная программа по предоставлению государственных и муниципальных услуг в электронной форме с использованием Интернета. Вместе с тем вопросы обеспечения информационной безопасности при реализации проектов электронного правительства на должном уровне не решаются: не вполне урегулированы вопросы обеспечения технологической и семантической совместимости государственных систем, недостаточно учитываются угрозы информационной безопасности в деятельности органов государственной власти и органов местного самоуправления, задерживается реализация Федерального закона «Об электронной подписи», существующее законодательство создает ограничения для трансграничного электронного взаимодействия.

Сохраняется технологическая зависимость России от ведущих производителей системного программного обеспечения (ПО). Создание национальной программной платформы на базе свободного ПО выявило ряд существенных проблем в обеспечении информационной безопасности. При этом недостаточна государственная поддержка российского производителя информационных технологий (ИТ) и технологий информационной безопасности.

В России разрабатывается и реализуется большое количество проектов, объединенных концепцией «Безопасный город». Результаты внедрения этих проектов требуют анализа с целью отбора наиболее эффективных решений для их последующего тиражирования. Уровень эффективности таких проектов может быть повышен за счет более широкого внедрения биометрических технологий идентификации личности, однако законодательство России ограничивает возможности использования таких технологий.

Правительство России планирует более активно использовать технологию «облачных» вычислений, для чего в первом квартале 2012 г. должен быть разработан соответствующий проект (концепция). Предполагается, что единый «облачный» сервис будет использоваться правительством, внебюджетными фондами, оборонной промышленностью, научно-технической и социальной сферой, а также средним и малым бизнесом. Во всем мире реализация таких сервисов сталкивается с проблемами правового регулирования отношений их пользователей. Однако разработка нормативного правового обеспечения для использования «облачных» технологий даже в рамках «электронного правительства» пока не осуществляется.

В настоящее время в России наблюдается «образовательная революция» – 57% граждан в возрасте 25-35 лет имеют высшее образование, и взрывной рост образовательных потребностей продолжается. Учитывая, что Россия стремится стать полноправным членом глобального информационного пространства, потребность в специалистах по информационной безопасности будет только увеличиваться. Однако отсутствие четкой стратегии кадрового сопровождения государственной программы Российской Федерации «Информационное общество (2011-2020 годы)» (не предусматривается научное обоснование масштабов подготовки таких специалистов в вузах России и совершенствование образовательных программ различного уровня) является сегодня серьезным сдерживающим фактором эффективного становления инновационной экономики.

Национальный форум информационной безопасности традиционно объединяет широкий круг специалистов, представляющих различные аспекты обеспечения информационной безопасности. Устремления участников форума направлены на формирование в России современной, высокоэффективной и безопасной информационно-коммуникационной инфраструктуры, создающей базу для развития информационного общества, в котором будет безусловно гарантирован суверенитет России и процветание граждан нашей страны, будет защищено достоинство каждого человека и обеспечено доверие в отношениях государства и общества.

Исходя из этих целей, по результатам обсуждения участниками форума были выработаны следующие рекомендации.

1. Общие рекомендации

1.1. Разработать стратегию информационной безопасности России и план ее реализации.

1.2. Сформировать эффективную институциональную структуру управления информационной безопасностью в России.

1.3. Принять программу комплексного и оперативного совершенствования нормативной правовой базы для внедрения в деятельность органов государственной власти, органов местного самоуправления, организаций новейших информационно-коммуникационных технологий (ИКТ) и обеспечения информационной безопасности личности, общества и государства, отвечающей современным вызовам и угрозам.

1.4. Утвердить в качестве приоритета государственной политики модернизации и в качестве критерия ее успешной реализации – продвижение российских высокотехнологичных продуктов и услуг (в том числе ИТ и систем информационной безопасности) на глобальном рынке.

1.5. Разработать государственную программу развития отечественного программного обеспечения, в которой интегрировать «Национальную программную платформу» и «Маршрутную карту развития российской индустрии разработки ПО», а также успешный опыт разработки известных на международном рынке продуктов российских компаний.

1.6. Обеспечить правовое регулирование комплексной защиты критически важных объектов, в том числе их информационной безопасности. Создать государственные центры мониторинга защищенности государственных информационных ресурсов.

1.7. Поддержать разработку и публичное обсуждение проекта Основных направлений государственной политики в области формирования культуры информационной безопасности и организовать проведение общенациональных акций, направленных на по-

вышение уровня информирования населения об угрозах информационной безопасности.

1.8. Поддержать усилия, предпринимаемые Россией по консолидации международного сообщества для обеспечения международной информационной безопасности.

1.9. В целях усиления защиты детей от насилия с использованием глобальных ИКТ ускорить ратификацию Российской Федерацией Конвенции Совета Европы о защите детей от сексуальной эксплуатации (принята в 2007 г.) и Факультативного протокола к Конвенции о правах ребенка, касающегося торговли детьми, детской проституции и детской порнографии (принятого Генеральной Ассамблеей ООН в 2000 г.).

1.10. Законодательно закрепить процедуры публичного обсуждения (общественной экспертизы), в том числе с привлечением профессиональных сообществ, проектов нормативных правовых актов с использованием электронных средств массовых коммуникаций.

2. В области предоставления электронных услуг населению и развития электронного документооборота

2.1. Внести изменения в таможенное законодательство в целях регулирования предоставления трансграничных услуг, в том числе услуг в области обработки информации и обеспечения информационной безопасности.

2.2. Ввести порядок оформления документов по внешнеторговым операциям на основе электронного документооборота.

2.3. Организацию предоставления государственных и муниципальных услуг в электронной форме сориентировать на модернизацию системы управления с использованием ИКТ, в том числе за счет сокращения количества межведомственных и внутриведомственных транзакций, необходимых для оказания государственных и муниципальных услуг и их документирования.

2.4. Подготовить или инициировать подготовку модельного закона для государств-участников СНГ, направленного на гармонизацию требований по осуществлению защищенного (с использованием криптографических средств) трансграничного электронного документооборота в различных сферах жизнедеятельности общества, в том числе в экономике и социальной сфере.

2.5. Обеспечить соответствие требований по безопасности персональных данных, содержащихся на электронном носителе Универсальной электронной карты (УЭК), требованиям Федерального закона «О персональных данных», международным стандартам по обмену идентификационной информацией и другим требованиям по обеспечению информационной безопасности, повысить публичность деятельности по выпуску, выдаче и обслуживанию УЭК.

2.6. Урегулировать на законодательном уровне требования к процессам идентификации и аутентификации субъектов правоотношений при предоставлении государственных и муниципальных услуг в электронной форме.

2.7. Завершить с участием профессионального сообщества формирование нормативной правовой базы для применения электронной подписи в различных правоотношениях.

2.8. Внести изменения в миграционное и трудовое законодательство, законодательство о безопасности и о персональных данных в части регламентации и более широкого использования технологий биометрической регистрации, в том числе дактилоскопии, в целях более точной идентификации субъектов правоотношений.

2.9. Разработать нормативно-правовую базу развития и практического использования технологий «облачных» вычислений. Обеспечить правовое регулирование применения «облачных» сервисов при предоставлении государственных и муниципальных услуг в электронной форме, в том числе определить права и обязанности участников отношений.

2.10. Провести публичное обсуждение и общественную экспертизу проекта Гражданского кодекса Российской Федерации в части его соответствия государственной стратегии предоставления услуг в электронной форме (в том числе государственных и муниципальных услуг) и развития электронного документооборота.

3. В области стандартизации

3.1. Развивать научную базу для выработки национальных стандартов и рекомендаций в сфере безопасности информационных технологий.

3.2. Ускорить работы по гармонизации национальных стандартов Российской Федерации (ГОСТ Р) и международных стандартов (ISO) в области ИТ и информационной безопасности. Обеспечить перевод и информирование специалистов о действующих и разрабатываемых международных стандартах в области ИТ и информационной безопасности.

3.3. С целью обеспечения интересов России принимать участие в разработке международных стандартов в области ИТ и информационной безопасности.

4. В области поддержки отечественного производителя ИКТ и выхода российских компаний на зарубежные рынки

4.1. Сформировать программу мер государственной поддержки высокотехнологичной продукции и услуг (включая применение беззалоговых финансовых механизмов поддержки экспортных контрактов, проведение маркетинговых исследований потенциала экспортно-ориентированных секторов российской экономики и перспективных зарубежных рынков, поддержку международной маркетинговой деятельности российских поставщиков информационных продуктов и услуг на глобальный рынок, обучение специалистов в области маркетинга, продаж, изучения иностранных языков; проведение PR-кампаний на ведущих зарубежных рынках).

4.2. Определить поддержку экспорта высокотехнологичной продукции и услуг, включая продукты и услуги в области информационной безопасности, в качестве одного из приоритетов деятельности Комиссии при Президенте Российской Федерации по модернизации и технологическому развитию экономики России.

4.3. Создать системы мотивации коммерческих предприятий к поддержанию необходимого уровня безопасности своих информационных систем.

4.4. Стимулировать использование ИКТ в коммерческих организациях путем ускоренной амортизации ИКТ или выведения расходов на ИКТ из налогооблагаемой базы при расчете налога на прибыль.

4.5. Обеспечить правовое регулирование упрощенного порядка заключения и осуществления электронных сделок с использованием Интернета, в том числе путем принятия Федерального закона «Об электронных сделках».

4.6. Осуществить меры по противодействию демпингу со стороны зарубежных производителей из числа ИТ-компаний, практикующих внутрифирменное кросс-финансирование, в случае, если существует российский аналог импортируемого программного обеспечения.

4.7. В целях поддержки российских высокотехнологичных компаний, занимающихся исследованиями и разработками в области программного и специализированного аппаратного обеспечения, внести изменения в Федеральный закон «Об экспортном контроле», направленные на максимальное упрощение процедуры ввоза/вывоза партий и отдельных единиц высокотехнологичных товаров на сумму до 300 000 рублей.

5. В области противодействия преступности в информационной сфере

5.1. Рекомендовать АРБ и Ассоциации банков «Россия» совместно с Банком России разработать методические рекомендации по противодействию хищению денежных средств клиентов с использованием дистанционного банковского обслуживания (ДБО).

5.2. Рекомендовать Банку России совместно с заинтересованными федеральными органами исполнительной власти разработать единый порядок блокирования похищенных средств клиентов банков и последующего их возврата.

5.3. Внести изменения в законодательство Российской Федерации в части квалификации преступлений, связанных с системами ДБО, определении времени и места завершения преступления, а также в части предоставления кредитной организацией справок по операциям и счетам юридических лиц и граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, органам внутренних дел при осуществлении ими функций по выявлению, предупреждению и пресечению любых преступлений, осуществляемых с использованием ИКТ.

5.4. Учитывая, что с развитием информационно-коммуникационных технологий (ИКТ) любое правонарушение может осуществляться с применением ИКТ, оценить целесообразность установления самостоятельных норм уголовной и административной ответственности за традиционные правонарушения, совершенные с применением ИКТ.

6. В области подготовки кадров

6.1. Инициировать меры государственного стимулирования инвестиций бизнеса в дополнительное профессиональное образование в области ИТ и информационной безопасности на основе частно-государственного партнерства.

6.2. Предусмотреть специальный раздел государственной программы «Информационное общество (2011-2020 годы)», посвященный реализации первоочередных мероприятий, направленных на совершенствование подготовки, переподготовки и повышения квалификации специалистов в области ИТ и информационной безопасности, а также на формирование культуры информационной безопасности в обществе.

6.3. Рекомендовать Минобрнауки России, Рособрнадзору совместно с заинтересованными федеральными органами исполнительной власти и объединениями работодателей разработать меры по усилению контроля за качеством подготовки специалистов в области ИТ и информационной безопасности.

6.4. Рекомендовать Оргкомитету Инфофорума проработать организационные механизмы и методическое обеспечение для оценки потребности рынка в специалистах в области обеспечения информационной безопасности, повышения квалификации таких специалистов и добровольной сертификации их компетенции.

7. *В области развития деятельности Инфофорума*

Рекомендовать Оргкомитету Инфофорума усилить аналитическую, проектную и консультативную составляющие в деятельности форума.

Электронное государство развивается

Организаторы 7-ой Всероссийской конференции «E-government-2012. Информационное общество: современная инфраструктура и технологии государственного управления» – компания Infor-media Russia совместно с Российским Агентством развития информационного общества (РАРИО). Участники – главы федеральных департаментов, министры субъектов Российской Федерации, непосредственно связанные с применением информационных технологий в практике государственного управления, а также другие специалисты в данной области. Главные темы мероприятия: реализация Государственной программы «Информационное общество 2011-2020 гг.», повышение эффективности функционирования электронного правительства, системы межведомственного электронного взаимодействия и взаимодействия региональных и муниципальных органов власти с гражданами и другие аспекты информационных технологий государственного управления.

Материалы конференции читайте в № 3 нашего журнала.

