ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ВАЖНЫЙ ФАКТОР ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СТРАНЫ

МИНИСТР РОССИЙСКОЙ ФЕДЕРАЦИИ ПО СВЯЗИ И ИНФОРМАТИЗАЦИИ
Леонид Дододжонович Рейман

Вопросы построения информационного общества в свете развития современных технологий и глобализации экономики становятся как никогда актуальными. Все больше жителей Земли связываются друг с другом с помощью инфокоммуникаций. Происходит необратимый поворот к сетевой экономике, основанной на передаче и обработке информации. Именно по качеству обеспечения информационных и телекоммуникационных услуг судят об экономическом потенциале государства.

Сегодня достижения в сфере обеспечения качества работы информационной, телекоммуникационной техники и различных систем передачи информации наблюдаются во всех составляющих отрасли связи и информатизации. Она является одной из наиболее перспективных и динамично развивающихся базовых инфраструктурных отраслей, обладающих потенциалом долгосрочного роста. Основным движущим фактором данной отрасли является развитие рынка услуг связи и информатизации, однако наряду с удовлетворением потребностей общества одной из основных ее задач является обеспечение национальной безопасности.

Преобразования, проводимые в отрасли связи и информатизации в 2002 году, позволили сохранить в течение последних лет устойчивую тенденцию роста предоставления услуг – на 35–40% в год. Так, населению в 2002 году было предоставлено услуг связи на сумму 270 млрд. руб., что на 39,5% выше показателей 2001 года. Количество телефонных аппаратов на 100 жителей России возросло до 25. Налоговые платежи отрасли в консолидированный бюджет страны составили 60,3 млрд. руб. (т.е. увеличились на 21,8% по сравнению с прошлым годом).

В конце 2002 года была принята в первом чтении новая редакция Федерального закона «О связи». Он направлен на создание правил взаимодействия участников телекоммуникационного рынка и на обеспечение защиты прав пользователей услуг связи и создает необходимые предпосылки для модернизации сети и ускоренного развития новых технологий.

В 2002 году стартовал первый этап Федеральной целевой программы «Электронная Россия». Она стала катализатором развития инфокоммуникационных технологий в стране. Для развития технологий «электронного правительства» проведен анализ телекоммуникационной инфраструктуры и автоматизированных систем бюджетных организаций, разработана концепция электронного документооборота в органах государственной власти, отработаны технические решения в регионах России по обеспечению массового доступа граждан к сети Интернет на основе использования общедоступных сетей школ и почтовых отделений связи.

Новые технологические возможности все активнее проникают в нашу жизнь. Впервые в России апробированы технологии сотовой связи третьего поколения, обеспечивающие абонентам расширенный набор услуг, включая доступ к сети Интернет и мультимедиа. Начались пробные передачи наземного цифрового телевещания, организованные на базе отечественного оборудования.

Успешно осуществляется программа по обновлению и расширению российской спутниковой группировки гражданского назначения.

Важнейшими итогами работы отрасли в минувшем году стали и такие важные мероприятия, как восстановление инфокоммуникационной инфраструктуры в Чеченской Республике, а также в районах Дальнего Востока и южных регионах, пострадавших от стихийных бедствий.

Основными задачами отрасли в 2003 году являются: совершенствование тарифной политики и законодательной базы отрасли, в частности, разработка концепции информационной безопасности сети связи общего пользования, обеспечение существенного прогресса в развитии передовых технологий и создании благоприятного инвестиционного климата.

В свою очередь решение этих задач будет способствовать повышению национальной безопасности Российской Федерации, в том числе и информационной безопасности.

Проблемы информационной безопасности многогранны и включают в себя все аспекты обеспечения безопасности, как на отдельном рабочем месте, так и в функционировании глобальных систем и сетей связи.

Доктриной информационной безопасности Российской Федерации определено, что одной из составляющих национальных интересов Российской Федерации в информационной сфере является защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

Для выполнения поставленных задач в 2002 году был введен в действие Федеральный закон «Об электронной цифровой подписи», направленный на решение проблемы обеспечения правовых условий для использования электронной цифровой подписи в процессах обмена электронными данными, при соблюдении которых электронная цифровая подпись признается юридически равнозначной подписи физического лица. Законом предусмотрена защита прав лиц, использующих электронную цифровую подпись в процессах электронного обмена данными. В целях защиты информационных систем государственных структур законом установлено обязательное использование в них только сертифицированных средств электронной цифровой подписи.

В целях реализации данного закона в настоящее время ведется работа по формированию инфраструктуры, обеспечивающей использование Закона «Об электронной цифровой подписи», и разработке соответствующих нормативных документов.

Особенного внимания заслуживает проблема подключения к глобальным открытым компьютерным сетям, и в первую очередь к Интернету. Этот процесс следует рассматривать через призму информационной безопасности, которая является составной частью национальной безопасности. Политика использования информационных ресурсов Интернета, будучи открытой, должна в обязательном порядке предусматривать защиту сетевого оборудования от проникновения в него скрытых элементов информационного воздействия.

В настоящее время прорабатывается вопрос о составе нормативно-правовых актов, регулирующих вопросы защиты информации при подключении информационных систем и информационных ресурсов к сети Интернет, взаимодействие интернет-провайдеров с правоохранительными органами в борьбе с компьютерной преступностью.

Трудно оценить ущерб, если выводится из строя стратегически важный сегмент информационной инфраструктуры страны. Как показывают последние политические события, все чаще массированные атаки хакеров используются с целью блокирования, взлома интернет-сетей.

Это вызывает повышенную обеспокоенность, особенно по поводу уязвимости перед возможной компьютерной атакой на системы жизнеобеспечения, засекреченные источники информации как со стороны злоумышленников-одиночек, так и технически грамотных террористов.

В этой связи следует особо подчеркнуть, что противоборство с киберпреступниками приобретает новые формы, перемещаясь в сферу Интернета и высоких технологий. Развитые государства, широко использующие компьютерную связь и высокотехнологичные системы, могут легко оказаться жертвой массированного компьютерного удара со стороны противоборствующих сил, способного резко дестабилизировать ситуацию. Поэтому проблеме защиты систем и сетей связи придается особенно важное значение.

Мы уже имеем ряд конкретных поручений, в соответствии с которыми ведем разработку вопросов защиты критических объектов телекоммуникационной инфраструктуры.

Совершенно очевидно, что успех в этой области во многом зависит от тех технических возможностей, которые мы можем предоставить на законном основании в распоряжение правоохранительных органов для обеспечения их деятельности, не нарушая, естественно, конституционных прав личности, гражданина.

На этом направлении еще предстоит проделать большой объем работы по пересмотру нормативно-правовой базы в данной области, не вполне соответствующей современным условиям.

Решение проблемы обеспечения информационной безопасности существенно осложняется широким использованием на сетях связи России средств связи зарубежного производства, программное обеспечение которых зачастую поставляется без исходных текстов, что создает возможность внедрения в программу недекларируемых функций, например, закладок.

К этому необходимо добавить, что не только проводные и подвижные средства связи, но и отечественные космические аппараты российской орбитальной группировки спутников связи и вещания в последнее время оснащаются в основном средствами связи иностранного производства.

На отечественный телекоммуникационный рынок выходят зарубежные системы глобальной подвижной спутниковой связи, управление космическими группировками которых осуществляется из центров, размещенных за рубежом.

Универсальность, скрытность, многовариантность форм программно-аппаратной реализации, радикальность воздействия, широта выбора места и времени применения, экономичность делают информационное воздействие чрезвычайно опасным. Оно легко маскируется под средства защиты и позволяет вести наступательные действия без объявления войны.

Для обеспечения безопасности и конфиденциальности в киберпространстве необходимо, чтобы угрозы были определены и предотвращены, а способность правоохранительных органов локализовать и определить преступников в сфере высоких технологий увеличивалась.

В соответствии с Федеральным законом «О противодействии экстремистской деятельности», концепция информационной безопасности сети связи общего пользования предусматривает разработку обязательных для выполнения операторами связи механизмов противодействия экстремистской деятельности.

Таким образом, в центре внимания министерства остается работа по минимизации возможных негативных последствий, в первую очередь путем проведения политики, которая стимулирует применение передовых технологий и в то же время способствует развитию отечественных информационных и телекоммуникационных технологий, производства технических и программных средств, не уступающих мировому уровню.

Учитывая, что в современных коммутационных и управляющих системах, а также во вспомогательных средствах, которыми оснащаются узлы связи и управляющие структуры организаций связи, основными компонентами являются микропроцессорные системы с поддерживающим программным обеспечением, особую значимость для объектов электросвязи приобретает возможность предупреждения опасного воздействия на них вредоносных программ-вирусов.

К сожалению, программно-аппаратные средства связи и вспомогательных систем не сертифицируются по требованиям информационной безопасности, не регламентируется порядок использования специализированных защитных программ. К тому же на сегодняшний день такие требования еще и не разработаны.

Однако совершенно очевидно, что решение вопросов информационной безопасности требует комплексного подхода, включая создание соответствующих структур и подготовку кадров. С мая 1999 года в Московском и Санкт-Петербургском университетах связи и информатики открылась новая специальность – «Защищенные системы связи». В настоящее время по этому профилю обучается порядка 200 студентов. В системе ИПК периодически проводятся семинары, издаются учебные пособия по данной тематике.

Еще одной важной проблемой является то, что появившиеся в последнее время на информационном рынке и распространяемые всевозможными коммерческими структурами самые разнообразные базы данных, содержащие информацию государственной телефонной сети, персональные данные и тому подобные информационные ресурсы, не защищены должным образом ни в правовом, ни в техническом плане. В этой связи должно быть уточнено понятие собственности на информационные ресурсы и конкретизированы правовые механизмы обеспечения соответствующих прав собственности.

Такое положение объясняется прежде всего отсутствием необходимой нормативно-правовой базы, а также организационной структуры, осуществляющей координацию работ в области обеспечения информационной безопасности сетей связи общего пользования, анализ уязвимых мест и выработку рекомендаций по их защите, а также сертификацию и аттестацию средств систем и сетей связи на соответствие требованиям информационной безопасности.

Таким образом, важнейшей составляющей информационной инфраструктуры страны, обеспечивающей потребности управления государством, обороны, безопасности, охраны правопорядка, экономики страны, а также потребности физических и юридических лиц в услугах связи, является ЕСС России. В связи с этим обеспечение информационной безопасности ЕСС России играет решающую роль в обеспечении национальной безопасности страны.

В России для эффективного решения задач, стоящих перед отраслью, должна быть сформирована система обеспечения информационной безопасности ЕСС России. В основу этой системы должна быть положена Концепция обеспечения информационной безопасности сетей связи общего пользования.

Проект российской концепции уже рассмотрен НТС Минсвязи России и в настоящее время дорабатывается. Мне представляется целесообразным скорейшее ее согласование, утверждение и внедрение в жизнь.

Всесторонне взвешенная, продуманная концепция, научно-обоснованный план ее внедрения являются дальнейшим развитием положений Доктрины информационной безопасности Российской Федерации в области инфокоммуникаций. Она будет включать вопросы совершенствования правового, методического, научно-технического и организационного обеспечения информационной безопасности сетей связи.

В заключение хотелось бы подчеркнуть, что определяющим фактором успешного решения задач обеспечения информационной безопасности будет являться тесное взаимодействие и сотрудничество граждан, бизнеса и органов государственной власти.