

ИНФОБЕЗОПАСНОСТЬ РОССИИ в цифровую эпоху

Л.Павлова

DOI: 10.22184/2070-8963.2018.71.2.36.37

Под таким девизом проходил 20-й Большой национальный форум информационной безопасности – "Инфофорум-2018". Что хорошо объяснимо: в условиях цифровой экономики бесперебойное функционирование государственных и частных информационных систем, критической информационной инфраструктуры, телекоммуникационных сетей, а также стабильная работа интернета, защищенность корпоративных и персональных данных станут залогом развития экономики и безопасности государства в целом.

Заявленная "Инфофорумом-2018" тема напрямую связана с реализацией программы "Цифровая экономика РФ". Как подчеркнул в своем выступлении Олег Духовницкий, руководитель Федерального агентства связи, эпоха цифровой экономики приведет к кардинальной модернизации инфраструктуры в большинстве отраслей, и в первую очередь в отрасли телекоммуникаций. В части информационной инфраструктуры цифровой экономики Россвязь является одним из исполнителей базового направления программы по значимым для развития всей ИКТ-отрасли мероприятиям, среди которых: формирование основных положений развития единой сети электросвязи РФ на перспективу до 2024 года; разработка генеральной схемы развития сети связи РФ; обеспечение функционирования услуги ШПД в населенных пунктах с численностью населения от 250 до 500 человек; разработка предложений по внесению изменений в стандарты и спецификации, необходимые для построения спутникового сегмента и сетей 5G; разработка генеральной схемы развития инфраструктуры хранения и обработки данных, включающей государственный и корпоративный сегмент, и др. В ходе работы по реализации этих задач Россвязь будет уделять особое внимание вопросам обеспечения информационной безопасности, подчеркнул О.Духовницкий. В первую очередь это касается обеспечения единства, устойчивости и безопасности информационно-телекоммуникационной инфраструктуры РФ на всех уровнях информационного пространства.

Как отметил в своем выступлении председатель комитета Госдумы по информационной политике, информационным технологиям и связи Леонид Левин, нынешний год станет прорывным в реализации принятой правительством в 2017 году программы развития цифровой экономики в стране. В планах правительства – вынесение на рассмотрение Госдумы более 50 законопроектов, направленных на обеспечение процесса построения цифровой экономики. Особое место в этой программе занимает направление информационной безопасности, включающее защиту личности, учет национальных интересов в международных документах по теме информационной безопасности, экспорт в сфере информационной безопасности, создание системы повышения информационной грамотности граждан.

Согласно планам, в стране должна развиваться система стимулов приобретения российских программных, технических и сервисных продуктов. К 2020 году доля внутреннего сетевого трафика российского сегмента Сети, маршрутизируемого через иностранные серверы, должна составить не более 35%; не более 30% должна составить стоимостная доля закупаемого или арендуемого органами власти и компаниями с государственным участием иностранного ПО (еще недавно эта доля составляла более 90%); не менее 20% должна составить доля субъектов информационного взаимодействия, использующих стандарты безопасного информационного взаимодействия в области IoT. "Важно, чтобы эти показатели

не превратились в пустые цифры, иначе ради формального достижения показателей запретительными мерами мы можем разрушить хрупкую систему сетевых рынков и подорвать конкурентоспособность отечественного бизнеса, – отметил Л. Левин. – Ключевую роль должны сыграть экспертные обсуждения на парламентских площадках и принятие мер регулирования, обеспечивающих интересы государства и общества в долгосрочной перспективе”.

В этом отношении определенный опыт уже есть, он связан с разработкой и принятием закона № 187-ФЗ “О безопасности критической информационной инфраструктуры Российской Федерации”, действующего с 1 января этого года. Закон определил права, обязанности и ответственность лиц, которые владеют объектами критической информационной инфраструктуры (КИИ), а также операторов связи и информационных систем, обеспечивающих взаимодействие этих объектов. Нормативно-правовое регулирование и государственный контроль за выполнением нового закона возложены на Федеральную службу по техническому и экспортному контролю (ФСТЭК России). Виталий Лютиков, заместитель директора ФСТЭК России, отметил, что документ оказался сложным для разработки, поскольку это – “первый практический опыт выработки критериев ущерба для безопасности государства в различных сферах и отраслях деятельности”. Однако принятие закона поможет государству обязать бизнес выделять больше денег на обеспечение информационной безопасности для всей критической информационной инфраструктуры; а реализация нового закона позволит снизить киберугрозы для организаций – владельцев КИИ.

По словам В. Лютикова, будет издано как минимум 18 подзаконных нормативных актов, наиболее важным из которых является постановление правительства, утверждающее критерии значимости объектов критической информационной инфраструктуры. В настоящий момент проект находится на рассмотрении в аппарате правительства. После утверждения

можно будет приступить к первому шагу – определению объектов, в отношении которых выдвигаются требования регулятора и осуществляется государственный контроль за обеспечением безопасности. ФСТЭК уже разработала требования по безопасности значимых объектов КИИ и требования к системам обеспечения безопасности, которые должны создаваться субъектами.

Одна из критически важных для функционирования экономики систем – финансовая. Банк России занялся вопросами обеспечения информационной безопасности отечественной банковской сферы еще 15 лет назад и добился значительных успехов, отметил на “Инфофоруме-2018” замначальника главного управления безопасности и защиты информации ЦБ РФ Артем Сычев. В целях повышения уровня обеспечения информационной безопасности кредитно-финансовые организации могут обязать проходить проверку на реальную защищенность своих систем не менее одного раза в год. По словам А. Сычева, соответствующую норму Центробанк планирует утвердить в новой редакции Положения № 382-П “О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств”. Документ согласован с ФСТЭК России, одобрен Советом директоров Банка России и находится на согласовании в ФСБ России.

В свою очередь, ФСБ России планирует в ближайшее время опубликовать для общественного обсуждения проекты нормативных правовых актов для реализации закона о критической информационной инфраструктуре. ■

Обсуждение тем, затронутых на 20-м Большом национальном форуме информационной безопасности “Инфофорум-2018”, будет продолжено в ходе региональных, тематических и международных конференций Инфофорума в 2018 году.