
Юрчук В.С., Балванович А.В. Риски снижения качества услуг связи в связи с изменением федерального законодательства [Электронный ресурс] // Информационно-экономические аспекты стандартизации и технического регулирования: Научный интернет-журнал, 2017. – № 2(36). – Режим доступа: http://iea.gostinfo.ru/files/2017_02/2017_02_03.pdf.

УДК 341.231.4

РИСКИ СНИЖЕНИЯ КАЧЕСТВА УСЛУГ СВЯЗИ В СВЯЗИ С ИЗМЕНЕНИЕМ ФЕДЕРАЛЬНОГО ЗАКОНОДАТЕЛЬСТВА

Юрчук В.С. канд. юрид. наук, доц., НОУ ВПО «Московский Университет имени С.Ю. Витте».

Балванович А.В. студент, НОУ ВПО «Московский Университет имени С.Ю. Витте».

В статье рассматриваются риски снижения качества услуг связи в связи с изменением федерального законодательства, а также на основании мнения экспертного сообщества предлагается комплекс мероприятий по их снижению.

Ключевые слова: частная жизнь, персональные данные, риски, изменение законодательства.

UDC 341.231.4

RISKS OF REDUCING THE QUALITY OF COMMUNICATION SERVICES DUE TO CHANGES IN FEDERAL LEGISLATION

Yurchuk V.S. cand. jurid. Sciences, NOU VPO «Moscow University named S.Y. Witte »

Balvanovich A.V. student, NOU VPO «Moscow University named S.Y. Witte»

The article deals with the risks of reducing the quality of telecommunications services due to changes in federal legislation, and a set of measures to reduce them is proposed based on the opinion of the expert community.

Keywords: private life, personal data, risks, change of legislation.

Как отмечается в ГОСТ Р 53724-2009 «Качество услуг связи. Общие положения». «Качество услуг связи – это степень соответствия присущих услугам связи характеристик требованиям, установленным нормативными

документами» [5]. Одним из ключевых элементов качества услуг, является обеспечение сохранности передаваемых пользователями данных. В связи с этим представляется целесообразным рассмотреть вопрос предполагаемого влияния изменений в законодательстве РФ на качество услуг связи.

С 1 июля следующего года вступят в силу положения, ориентированные на противодействие терроризму и обеспечение общественной безопасности, которые в обиходе получили название «закона Яровой», по имени наиболее яркого инициатора принятия данных изменений заместителя председателя Государственной думы Ирины Анатольевны Яровой. Отмеченные положения представлены двумя Федеральными законами:

Первый ФЗ ориентирован на ужесточение уголовной ответственности за преступления террористической направленности (Федеральный закон от 6 июля 2016 г. № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» [3]).

Второй на усиление иных мер, ориентированных на борьбу с терроризмом (Федеральный закон от 06 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»). [4]

В связи с принятыми нововведениями «юридическим лицам, а также индивидуальным предпринимателям, оказывающим услуги связи на основании соответствующей лицензии» [1] предписано хранить на территории Российской Федерации различные виды сообщений пользователей связи (текстовые, голосовые, изобразительную, аудио, видео и др.). При этом период хранения данной информации может достигать 6 месяцев. Эти же нововведения касаются и организаторов распространения информации в

Интернете. «Организатором распространения информации в сети «Интернет» является лицо, осуществляющее деятельность по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети «Интернет». [2]

Принятие приведенных выше Федеральных законов породило интенсивную полемику, как среди рядовых граждан, так и среди представителей профессионального сообщества. По мнению экспертов, их реализация может столкнуться с множеством затруднений. Изменения затрагивают всех без исключения граждан России, при этом его реализация ложится на плечи профильных частных и государственных предприятий. Интернет-омбудсмен, член экспертного совета «Агентства стратегических инициатив» Дмитрий Николаевич Мариничев отмечает, что при разработке отмеченных нововведений консультирование с экспертным сообществом не осуществлялось.

Экспертами в области связи и массовых коммуникаций высказывается мнение о проблематичности корректной реализации требований положений. Весь комплекс замечаний можно обобщенно разделить на пять основных направлений.

Первое направление вызвано повышением рисков, связанных с необходимостью длительного хранения информации. Возможность несоблюдения правил хранения касается в том числе и информации ограниченного доступа. Организации предоставляющие услуги связи могут осуществлять взаимодействия с множеством предприятий в различных областях. Например, предоставление услуг связи банкам, адвокатам, любой семье, т.е. предприятия в ходе осуществления своей профессиональной деятельности вынуждены осуществлять оборот информации охраняемой законодательством.

В настоящее время в Реестре лицензий в области связи Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций содержатся данные о 36 307 лицензиях. [6]

Наибольшая вероятность возникновения рисков, связанных с оборотом, охраняемой законом информации, заключается в том, что она может храниться у лиц, которые не могут это реализовать на требуемом уровне. Например, малые предприятия, предоставляющие услуги связи для ТСЖ и т.п.

Второе направление связано с имеющимся дефицитом технических средств обеспечения безопасности хранимых данных. Организаторами распространения информации в Интернете, а также средствами обмена сообщениями в первую очередь являются, электронная почта и социальные сети. Однако, сюда же можно отнести и сетевые игры с функцией обмена моментальными либо голосовыми сообщениями. По мнению экспертов Mail.Ru Group, среди разработчиков-администраторов подобного рода игр присутствует существенная доля малых инновационных предприятий, где количество сотрудников варьируется от 3 до 5 человек, кроме того они могут осуществлять свою деятельность на арендованном оборудовании. Следовательно и привлечение эксперта в области информационной безопасности не является для них приоритетным. При этом, рассматриваемые нами изменения в законодательстве предписывают хранить значительные объемы информации. Также, для реализации нововведений необходимо будет провести усовершенствовать оборудование. «Директор Департамента управления регуляторными рисками ПАО МТС Андрей Рого отмечает, что по оценке ПАО МТС – для того, чтобы реализовать положения закона, потребуется как минимум в 1 тыс. раз увеличить объемы хранилищ, которые на сегодняшний день существуют».[7]

Третье направление связано с качеством кадрового состава организаций связи. Данные, находящиеся под защитой законодательства будут расположены в специальных хранилищах, которые в свою очередь должны

обслуживать соответствующий персонал, обычные граждане. При этом в окружающей нас социально-экономической действительности нельзя гарантировать, что жизненные обстоятельства и личные интересы не будут превалировать над общественными, и хранимые данные не будут «просачиваться». Уточнение прав и обязанностей, а также ответственности данных специалистов в связи с нововведениями не производится.

Четвертое направление связано с возможностью активного поиска отечественными пользователями средств обмена сообщениями среди зарубежных сервисов. Реализация нововведений формирует потребность в увеличении расходов среди операторов связи и организаторов распространения информации без существенного повышения качества либо функционала предоставляемых услуг. Это в свою очередь скажется на стоимости оказания услуг, в направлении их увеличения. Следовательно, пользователи будут вынуждены искать менее затратные сервисы. Иными словами, нововведения могут привести к обратному эффекту, при котором: «во-первых, доступ к информации об отечественных пользователях получат зарубежные силовые ведомства, во-вторых, российские правоохранительные органы, осуществляющие деятельность по борьбе с терроризмом, отмеченный доступ утратят». Кроме того, основная масса информационно-телекоммуникационного оборудования, требуемого для реализации предписаний производится за рубежом. Иными словами, средства, направленные на закупку оборудования, будут поддерживать иностранного производителя. Даже при условии принятия решения о локализации хранилищ под управлением государства, по мнению экспертов «Ростеха» «жесткие, твердотельные и ленточные накопители предлагается продолжать закупать за рубежом» [8].

Четвертое направление связано высокой долей вероятности повышения стоимости требуемого информационно-телекоммуникационного оборудования. Рассматриваемые нами изменения в федеральном

законодательстве приведет к повышению спроса на данное оборудование, как следствие цена предложения будет увеличена. Это в свою очередь может негативно сказаться на всей отрасли уже в ближайшей перспективе.

Вместе с тем, даже при условии наличия приведенных выше рисков, профильные организации, осуществляющих свою деятельность в области предоставления услуг связи, будут ориентированы в первую очередь на реализацию формальной стороны нововведений, что не всегда может содействовать повышению уровня безопасности при хранении данных. Иными словами, вероятность возникновения рисков, связанных со снижением качества предоставления услуг связи значительно, повышается.

С целью устранения либо минимизации приведенных выше рисков экспертами в рассматриваемой нами области предлагаются к реализации следующие мероприятия.

Во-первых, представляется целесообразным осуществление пилотного проекта. Пилотный проект позволит конкретизировать, какие именно финансовые ресурсы следует привлечь и какое оборудование следует приобрести, а также порядок взаимодействия с соответствующими ведомствами при работе с такими объемами данных.

Во-вторых, сократить объем требуемых для хранения данных в временном плане. Т.е. начать сохранение производимой информации, например, с месяца и затем постепенно наращивать временной интервал.

В-третьих, представляется целесообразным осуществление государственного контроля стоимости оборудования необходимого для реализации нововведений. Это позволит сдержать рост цен со стороны производителей, а также более системно подходить к бюджетному планированию предприятий сектора связи. При этом следует отметить, что «локализация оборудования и программного обеспечения, необходимого для исполнения антитеррористических поправок, обойдется в 10,3 млрд руб., следует из предварительных подсчетов «Ростеха» [8].

В-четвертых, специализированные хранилища данных должны быть сформированы соответствующими государственными органами и находиться в их ведомстве. Отмеченные действия сформируют необходимые условия для минимизировать риск и утечки охраняемой законом информации, в том числе и посредством отстранения от обслуживания данных хранилищ низкоквалифицированного персонала.

В-пятых, для устранения противоречия между фиксированными нормами закона, подзаконных актов, и непрерывным прогрессом информационных технологий, предлагается шире использовать механизм ссылки на стандарты в нормативных правовых актах, что позволит повысить эффективность данного пакета законов и снизить их негативные последствия за счет реализации в стандартах консенсусной позиции, отражающей мнения всех заинтересованных сторон [9-14].

Реализация приведенных выше положений позволит найти компромисс между потребностями граждан в качестве предоставления услуг связи, сохранностью данных, стоимости услуг, профессиональным сообществом, государством в области безопасности.

Список использованных источников и литературы

1. Федеральный закон от 07.07.2003 № 126-ФЗ (ред. от 06.07.2016) «О связи» // Собрание законодательства РФ, 14.07.2003, № 28, ст. 2895. – <http://www.consultant.ru/>
2. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 01.01.2017) «Об информации, информационных технологиях и о защите информации» // Парламентская газета, № 126-127, 03.08.2006. – <http://www.consultant.ru/>
3. Федеральный закон от 6 июля 2016 г. № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // Собрание законодательства РФ, 11.07.2016, № 28, ст. 4559
4. Федеральный закон от 06 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и

отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // Собрание законодательства РФ, 11.07.2016, № 28, ст. 4558;

5. ГОСТ Р 53724-2009 «Качество услуг связи. Общие положения». – Стандартиформ. М. – 2011;

6. Реестре лицензий в области связи Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций <http://rkn.gov.ru/communication/register/license/?all=1>;

7. Добрикова Е. «Закон Яровой», по мнению операторов связи, не гарантирует безопасность конфиденциальных данных абонентов» // <http://www.garant.ru/news/1095207/>;

8. Кантышев П. «Ростеху» нужно 10,3 млрд рублей на разработки для закона Яровой / Ведомости – <http://www.vedomosti.ru/technology/articles/2016/09/05/655653-rostehu-zakona-yarovoі>.

9. Докукин А.В., Коновалов В.А. Гармонизация потребностей и ожиданий сторон в нормотворческом процессе в области стандартов качества // Транспортное дело России. 2014. №5. С. 98-101.

10. Орлова Е.Е., Докукин А.В. Согласование интересов субъектов права в нормотворческом процессе в техническом регулировании // Транспортное дело России. 2014. № 3

11. Орлова Е.Е., Докукин А.В. Понятийный аппарат нормотворчества в техническом регулировании // Информационно-экономические аспекты стандартизации и технического регулирования. 2013. № 5 (15).

12. Докукин А.В. Необходимость гармонизации интересов производителей и потребителей в техническом регулировании // Информационно-экономические аспекты стандартизации и технического регулирования. 2011. № 3 (3).

13. Докукин А.В. Повышение качества информационного обеспечения мониторинга правотворчества и правоприменения// Информационно-экономические аспекты стандартизации и технического регулирования. 2013. № 6(16).

14. Докукин А.В. Правовые вопросы разработки и распространения стандартов // Информационно-экономические аспекты стандартизации и технического регулирования. 2011. № 4 (4).

© Юрчук В.С.
© Балванович А.В.