Людмила Николаевна Бокова
Заместитель председателя
Комитета Совета Федерации по конституционному
законодательству и государственному строительству
E-mail: Bokova78@yandex.ru

Вадим Константинович Максимов
Кандидат юридических наук
E-mail: maximvad@mail.ru

Развитие законодательства Российской Федерации в условиях обеспечения международной информационной безопасности сети Интернет*

Аннотация: *в статье исследуется процесс формирования правовой системы обеспечения международной информационной безопасности, а также системы информационной безопасности в рамках российского законодательства. Актуальность темы обусловлена высокими темпами развития глобального информационного пространства и информатизации всех сфер жизнедеятельности общества, непростой политической ситуацией, сложившейся на мировой арене. Выявляются правовые проблемы, оказывающие влияние на успешное формирование системы МИБ и модернизацию законодательства России в области информационной безопасности, формулируется ряд предложений, способствующих реализации государственной политики России в области МИБ.*

Ключевые слова: *информационная глобализация, информационное пространство, информационное общество, международная информационная безопасность, государственная политика Российской Федерации.*

Ljudmila Nikolaevna Bokova
Deputy Chairman of the Committee on constitutional legislation
and state construction of the Council of Federation

Vadim Konstantinovich Maximov
Candidate of legal sciences

Development of the Legislation of the Russian Federation in Terms of Ensuring the International Information Security the Internet

Annotation: *the article investigates the process of formation of the legal system of ensuring international information security, and information security system in the*

* Тезисы к выступлению на российско-германской научной конференции «Интернет в деятельности государственных органов: правовое регулирование и безопасность», 30 июня 2016 г.

framework of the legislation of the Russian Federation. The relevance of the stated topic is determined due to the high pace of development in the global information society and informatization of all spheres of the society's life activities, as well as the complicated political situation established in the world.

One identifies some legal problems affecting the successful formation of the system of international informative security and modernization of the legislation of the Russian Federation in the field of information security, formulates a number of proposals that contribute to the successful implementation of the state policy of the Russian Federation in the field of the international informative security.

Keywords: *information globalization, information space, information society, international information security, state policy of the Russian Federation.*

1. Основные тенденции развития международной информационной безопасности.

Стремительные темпы развития и проникновение во все сферы современной жизни глобальных информационных процессов, расширение информационного пространства предоставляют качественно новые возможности доступа к новой информации, накопленному массиву знаний и культурному наследию. Информационная глобализация способствует ускоренному развитию, распространению и внедрению научных открытий и технических инноваций независимо от расстояний, сокращая затраты времени и стоимость внедрения новых технологий, товаров и услуг.

Государственное управление активно реформируется как уровне отдельных стран, так и их региональных объединений. В целях обеспечения открытости и прозрачности управления расширяются формы электронного взаимодействия с гражданским обществом и перечень оказываемых дистанционно государственных и муниципальных услуг, многократно увеличивается востребованность облачных технологий хранения информации, повсеместно сокращается уровень «цифрового» неравенства.

Однако в условиях усиления социальной, политической и экономической взаимозависимости, расширения и углубления международных интеграционных связей между государствами, их региональными и глобальными союзами, международными организациями, транснациональными корпорациями и фондами информационная глобализация и стремительное развитие информационного общества, возможности трансграничного оборота информации в информационном пространстве, по существу «отменяющие» межгосударственные границы, представляют угрозу не только национальной, но и международной безопасности, многократно увеличивая риски использования достижений в информационной сфере в целях, противоречащих задачам поддержания мировой стабильности и безопасности, мирного разрешения международных споров и конфликтов, неприменения силы, невмешательства во внутренние дела суверенных стран, соблюдения прав и свобод человека.

Глобальная информатизация способствует росту киберпреступности, применению информационных технологий в террористических, криминальных и иных противоправных целях, детерминирует новые формы и способы ведения информационных войн, ведет к использованию информационных технологий для достижения геополитических, военно-политических и иных целей в ущерб международной безопасности и стратегической стабильности.

Современное содержание рисков и угроз глобальной информатизации во многом обусловлено возможностями сети Интернет, которые, к сожалению, используются не только для достижения благих целей, но и для формирования негативных установок у пользователей Сети, использующих ее для совершения общественно опасных действий в отношении конкретного лица или группы лиц, сообщества либо целого государства или иной системы. Еще большими возможностями располагают преступные организации и сообщества, а также государства или межгосударственные объединения. Основными целями посягательств становятся критические инфраструктурные системы, государственные и негосударственные информационные ресурсы, центры обработки и хранения данных, персональные компьютеры и иные индивидуальные системы обработки, хранения и передачи информации. Так, выход из строя либо уничтожение критической гражданской инфраструктуры может привести к губительным последствиям в обороне, экономике, здравоохранении и безопасности. Несанкционированный доступ к конфиденциальной информации, существенные объемы которой хранятся в сети Интернет, включая персональные данные граждан и сведения, составляющие государственную или иную тайну, может нанести значительный вред как конкретному человеку или сообществу, так и отдельному государству или группе государств, сопоставимый по масштабам с последствиями стихийного бедствия, катастрофы или военного конфликта, способный привести к политическим, экономическим и социальным потрясениям.

Таким образом, следует признать, что информационная сфера нуждается в повышенном внимании и защите, выработке новых подходов к решению задач по обеспечению информационной безопасности, формированию адекватного вызовам международного и национального законодательства. В нынешней ситуации представляется весьма конструктивной позиция Российской Федерации, согласно которой основой целью ее государственной политики является содействие установлению международного правового режима, направленного на создание условий для формирования системы международной информационной безопасности (далее – МИБ). «Основами государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года» (утв. Президентом РФ 24 июля 2013 г. № Пр-1753) международная информационная безопасность определяется как «состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры» (п. 6).

Создание системы МИБ, обеспечивающей эффективное противодействие использованию информационных технологий в неконструктивных асоциальных целях, предполагает делегирование государствами части своих традиционных функций и полномочий международным организациям с целью успешного решения как региональных (Шанхайской организации сотрудничества, Содружеству Независимых Государств, Союзному государству, Организации договора о коллективной безопасности, Евразийскому экономическому содружеству и др.), так и универсальных задач, например в формате ООН. При этом в области создания МИБ наша страна стратегически исходит из того, что основной тенденцией формирования правовых и организационных основ

МИБ является формирование комплексной системы МИБ на двустороннем, многостороннем, региональном и глобальном уровнях, что прямо записано в п. 10 (подп. «а») «Основ государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года».

В целях формирования системы МИБ в последние годы Российская Федерация продолжает активное взаимодействие по названным направлениям в рамках таких международных организаций, как БРИКС, ШОС, СНГ, ОДКБ и АТЭС.

Так, Итоговая декларация VI саммита БРИКС (июль 2014 г., г. Форталеза, Бразилия) содержит пункты о необходимости использования и развития информационно-коммуникационных технологий на основе международного сотрудничества, общепризнанных норм и принципов международного права, что имеет первостепенное значение для обеспечения мирного, безопасного и открытого цифрового и интернет-пространства (п. 49), и о намерении сотрудничать в области борьбы с киберпреступлениями, для чего предстоит выработать универсальный и имеющий обязательную юридическую силу международно-правовой документ при главенстве ООН, продолжить совместную деятельность по выявлению возможностей для осуществления совместных действий по решению общих проблем безопасности в сфере использования ИКТ. Одновременно поддержано российское предложение о совместной разработке соглашения между странами БРИКС о сотрудничестве в области международной информационной безопасности.

Дальнейшее развитие международно-правового сотрудничества в области формирования общих подходов к проблематике МИБ получило в форме двусторонних Соглашений о сотрудничестве в области обеспечения МИБ между Правительством Российской Федерации и Правительством Республики Беларусь (2013 г.), Правительством Республики Куба (2014 г.) и Правительством Китайской Народной Республики (2015 г.), а также Соглашения с Правительством Федеративной Республики Бразилия о сотрудничестве в области обеспечения международной информационной и коммуникационной безопасности (2010 г.).

В указанных Соглашениях стороны подтверждают необходимость дальнейшего развития взаимодействия в области использования информационно-коммуникационных технологий, отметив стремление формировать многостороннюю, демократическую и прозрачную международную систему управления информационно-коммуникационной сетью Интернет в целях его реальной интернационализации и обеспечения равных прав государств на участие в этом процессе, включая демократическое управление основными ресурсами информационно-коммуникационной сети Интернет и их справедливое распределение[1].

В этих же целях продвигается российская инициатива о необходимости разработки и принятия государствами — членами Организации Объединенных Наций конвенции об обеспечении международной информационной безопасности. Современные условия требуют формирования действенных механизмов

[1] Подробнее см.: *Полякова Т. А., Акулова Е. В.* Развитие законодательства в области обеспечения информационной безопасности: тенденции и основные проблемы // Право. 2015. № 3. С. 7–9.

интернационализации управления сетью Интернет и увеличения в этом контексте роли Международного союза электросвязи, общепринятых правил поведения в киберпространстве, содействия «развитию региональных систем и формированию глобальной системы международной информационной безопасности на основе общепризнанных принципов и норм международного права (уважение государственного суверенитета, невмешательство во внутренние дела других государств, неприменение силы и угрозы силой в международных отношениях, право на индивидуальную и коллективную самооборону, уважение прав и основных свобод человека)» (подп. «в» п. 12 «Основ государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года»).

2. Глобальные и местные вызовы и задачи для Российской Федерации в области обеспечения международной информационной безопасности.

В Российской Федерации адекватно воспринимается существование угроз МИБ и необходимость формирования эффективной системы международной информационной безопасности, совершенствования не только международного, но и внутреннего законодательства, актуализации научных исследований.

Описание основных, в том числе стратегических угроз в области МИБ, определение цели, задач и приоритетных направлений государственной политики Российской Федерации в области МИБ, а также механизмы их реализации представлены в «Стратегии национальной безопасности Российской Федерации» (утв. Указом Президента РФ от 31 декабря 2015 г. № 683), уже упомянутых «Основах государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года», «Доктрине информационной безопасности Российской Федерации» (утв. Президентом РФ 9 сентября 2000 г. № Пр-1895). Последнюю предполагается обновить с учетом новейших реалий, для чего Советом безопасности Российской Федерации подготовлен проект ее новой редакции, который 24 июня 2016 г. размещен для общественного обсуждения (с 25 июня по 5 июля текущего года) на сайте Совета безопасности.

С учетом того, что состояние МИБ определяет и ситуацию внутри Российской Федерации, можно смело констатировать, что указанные стратегические документы актуальны и для внутрироссийской политики в области обеспечения национальной информационной безопасности.

Так, согласно «Основам государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года» к основным угрозам относится «использование информационных и коммуникационных технологий:

а) в качестве информационного оружия в военно-политических целях, противоречащих международному праву, для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности;

б) в террористических целях, в том числе для оказания деструктивного воздействия на элементы критической информационной инфраструктуры, а также для пропаганды терроризма и привлечения к террористической деятельности новых сторонников;

в) для вмешательства во внутренние дела суверенных государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей или теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию;

г) для совершения преступлений, в том числе связанных с неправомерным доступом к компьютерной информации, с созданием, использованием и распространением вредоносных компьютерных программ».

Данные угрозы детализированы в положениях «Доктрины информационной безопасности Российской Федерации».

Осознание угроз позволяет обозначить основные национальные интересы в данной сфере, к которым можно отнести (на основе положений проекта Доктрины информационной безопасности):

а) соблюдение прав и свобод человека и гражданина в области получения и использования информации, включая неприкосновенность частной жизни при использовании информационных технологий, информационную поддержку участия граждан в управлении государством, политической жизни общества;

б) обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры Российской Федерации, включая критическую информационную инфраструктуру Российской Федерации и единую сеть электросвязи Российской Федерации, мирное и военное время;

в) развитие отрасли информационных технологий в Российской Федерации, а также совершенствование деятельности по разработке, производству и эксплуатации средств обеспечения информационной безопасности, оказания услуг в области обеспечения информационной безопасности.

В целях подержания озвученных интересов в условиях расширения областей использования информационных технологий и широчайших возможностей трансграничного оборота информации в информационном пространстве весьма актуальны задачи разработки и создания российских защищенных технологий хранения и обработки информации, программного обеспечения, в частности операционных систем, снижения зависимости функционирования российского сегмента сети Интернет от элементов его инфраструктуры, управляемых зарубежными компаниями, в том числе в рамках импортозамещения. Необходимо сократить отставание Российской Федерации от ведущих зарубежных государств в развитии конкурентоспособных информационных технологий и их использовании для создания продукции и услуг на их основе, в том числе оказываемых с помощью сети Интернет.

К другим важным задачам в рассматриваемой сфере относится создание правовых и экономических условий для снижения уровня «цифрового неравенства»[1], более развернутого применения информационных технологий, в том числе «облачных», в государственном управлении в целях повышения прозрачности деятельности органов государственной власти и местного самоуправления, роста качества официальных интернет-сайтов органов

[1] Подробнее о «цифровом неравенстве» и мерах по его минимизации см.: *Хомченко А. И.* Информационное общество: правовые проблемы в условиях глобализации : дис. ... канд. юрид. наук. М., 2014. С. 80–88.

государственной власти и доступности государственных и муниципальных услуг с помощью электронных сервисов, доступных в сети Интернет для всех групп населения.

При этом необходимо обязательно увязывать внедрение новых информационных технологий со строжайшим соблюдением требований информационной безопасности, обеспечивающих безусловную защиту информации, содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа.

Сбор, обработка, накопление, хранение, поиск информации, ее распространение и предоставление потребителю, создание и использование информационных технологий и средств их обеспечения, защита информации и прав субъектов, участвующих в информационных процессах, не могут происходить без участия государства. В противном случае попытки обеспечить достаточные и необходимые меры по обеспечению информационной безопасности не увенчаются успехом.

На эти процессы накладывают свой отпечаток действия ведущих зарубежных стран, а также террористических и экстремистских организаций по наращиванию возможностей, в том числе с использованием сети Интернет, по информационно-техническому воздействию на информационную инфраструктуру Российской Федерации, в том числе на критическую информационную инфраструктуру, усиление технической разведки в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса, использование информационно-психологического воздействия со стороны различных внешних и внутренних сил, направленных на дестабилизацию внутриполитической, социальной, межнациональной и религиозной ситуации в стране.

Продолжается совершенствование методов и форм компьютерной преступности, прежде всего в денежно-кредитной, валютной, банковской и иных сферах финансового рынка, увеличивается число инцидентов, связанных с нарушением законных прав граждан на защиту тайны связи, личной и семейной тайны, персональных данных при использовании информационных систем и сетей связи.

Не способствует улучшению ситуации отсутствие правовых норм, регулирующих межгосударственные отношения в информационном пространстве, и соответствующих международно-правовых механизмов поддержания стратегической стабильности, международного паритета и равноправного стратегического партнерства в этой сфере.

С учетом указанных вызовов должны определяться задачи Российской Федерации в поддержании международной информационной безопасности.

Вместе с тем, несмотря на наличие внешних и внутренних угроз, мы отдаем себе отчет, что усилия государства и общества по борьбе с угрозами и мерами по поддержанию национальных интересов должны сопровождаться поддержанием необходимого баланса с интересами развития информационного общества, национальной экономики, защитой прав и свобод граждан, в том числе конституционного права свободно искать, получать, передавать, производить и распространять информацию любым законным способом.

3. Краткий обзор законодательства Российской Федерации в сфере обеспечения информационной безопасности в Интернете и основные направления его совершенствования.

К законодательству Российской Федерации, составляющему основу регулирования отношений, возникающих при использовании сети Интернет, относятся:

а) по наиболее общим вопросам правового режима функционирования информационных сетей и их государственного регулирования: Конституция Российской Федерации; Гражданский кодекс Российской Федерации; Федеральный закон «Об информации, информационных технологиях и о защите информации»; Федеральный закон «О персональных данных»; Федеральный закон «О связи»; Федеральный закон «О средствах массовой информации»;

б) по иным вопросам, имеющим отношение к правовому режиму информации в Интернете и определению условий доступа к ней, следует отметить IV часть Гражданского кодекса Российской Федерации, Уголовный кодекс Российской Федерации, Кодекс Российской Федерации об административных правонарушениях, Бюджетный, Градостроительный, Земельный, Налоговый, Трудовой и иные кодексы, Закон Российской Федерации «О государственной тайне» и Федеральные законы: «О федеральной службе безопасности»; «Об оперативно-розыскной деятельности»; «О государственной охране»; «О полиции»; «О рекламе»; «О защите детей от информации, причиняющей вред их здоровью и развитию»; «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»; «Об обеспечении доступа к информации о деятельности судов в Российской Федерации»; «О Центральном банке Российской Федерации (Банке России)»; «Об организации предоставления государственных и муниципальных услуг» и мн. др.

Всего в базе действующих законодательных актов Российской Федерации можно найти свыше 500 законов, тем или иным образом затрагивающих вопросы использования сети Интернет, хотя в основном нормы этих законов регулируют использование возможностей Интернета в повседневной жизни граждан при доступе к информации, ее размещении и т. д.

Одновременно необходимо отметить важнейшие Указы Президента Российской Федерации, которые регулируют использование Интернета российскими органами государственной власти. Указом Президента Российской Федерации от 17 марта 2008 г. № 351 в целях обеспечения информационной безопасности Российской Федерации определены требования к использованию информационно-телекоммуникационных сетей, позволяющих осуществлять передачу информации через государственную границу Российской Федерации, в том числе при использовании международной компьютерной сети Интернет, в ходе оборота сведений, составляющих государственную либо служебную тайну.

В целях противодействия угрозам информационной безопасности России при использовании сети Интернет Указом Президента Российской Федерации от 22 мая 2015 г. № 260 предписано преобразовать сегмент международной компьютерной сети Интернет для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, находящийся в ведении Федеральной службы охраны, в российский государственный сегмент сети Интернет, обеспечивающей подключение к сети Интернет предназначенных для взаимодействия с ней государственных информационных

систем и информационно-телекоммуникационных сетей государственных органов и организаций, созданных для выполнения задач, поставленных перед федеральными государственными органами.

Между тем для более эффективного использования сети Интернет в интересах государственного управления и местного самоуправления необходимо разработать нормы, позволяющие четче разграничить требования к обработке общедоступной информации и информации, составляющей государственную или иную охраняемую законом тайну, детальнее урегулировать вопросы, связанные с использованием «облачных» технологий, в том числе в части обеспечения безопасности и конфиденциальности информации, передаваемой поставщику «облачных» услуг.

В силу глобальности информационного общества и развития трансграничных процессов важной задачей становится обеспечение безопасности персональных данных, используемых в различных информационных системах. В минувшем году путем внесения поправок в Федеральный закон «Об информации, информационных технологиях и о защите информации» созданы правовые основания решения проблемы размещения на зарубежных серверах информационных систем, используемых государственными органами, органами местного самоуправления, государственными и муниципальными унитарными предприятиями или государственными и муниципальными учреждения, что минимизирует риски несанкционированного уничтожения, блокировки, изменения информации на официальных сайтах.

Внесение изменений в Федеральный закон «О персональных данных» позволит обеспечить сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение персональных данных граждан Российской Федерации исключительно на территории Российской Федерации.

Вместе с тем полагаем, что работа по совершенствованию законодательства в сфере регулирования использования возможностей сети Интернет будет продолжена с учетом новых вызовов.

В заключение хотелось бы вновь обратить внимание на необходимость совершенствования законодательства в следующих проблемных областях:

– обеспечения информационной безопасности при использовании «облачных» технологий;

– создания всеобъемлющей системы безопасности критической информационной инфраструктуры;

– повышения эффективности и безопасности функционирования информационной инфраструктуры Российской Федерации, в том числе для устойчивого взаимодействия органов власти, недопущения внешнего контроля ее функционированием;

– совершенствования целостности, устойчивости функционирования и безопасности единой сети электросвязи Российской Федерации;

– создания правовых условий для повышения конкурентоспособности российских компаний инфокоммуникационной отрасли;

– выработки и реализации мер государственной поддержки организаций, осуществляющих деятельность по разработке, производству и эксплуатации средств обеспечения информационной безопасности, оказания услуг в области обеспечения информационной безопасности, а также организаций, осуществляющих образовательную деятельности в данной области;

– повышения уровня защиты персональных данных.

Полагаем, что совместными усилиями мы сможем обеспечить необходимые условия для создания и функционирования безопасной сети Интернет и всей инфокоммуникационной среды в настоящем и будущем.

Пристатейный библиографический список

1. О безопасности : федеральный закон РФ от 28 декабря 2010 г. № 390-ФЗ // Собр. законодательства Рос. Федерации – 2011. – № 1, ст. 2.

2. О государственной охране : федеральный закон РФ от 27 мая 1996 г. № 57-ФЗ // Собр. законодательства Рос. Федерации – 1996. – № 22, ст. 2594.

3. О государственной тайне : закон РФ от 21 июля 1993 г. № 5485-1 // Собр. законодательства Рос. Федерации. – 1997. – № 41, ст. 8220–8235.

4. О персональных данных : федеральный закон РФ от 27 июля 2006 г. № 152-ФЗ // Собр. законодательства Рос. Федерации – 2006. – № 31, ст. 3451.

5. О связи : федеральный закон РФ от 7 июля 2003 г. № 126-ФЗ // Собр. законодательства Рос. Федерации – 2003. – № 28, ст. 2895.

6. Об информации, информационных технологиях и о защите информации : федеральный закон РФ от 27 июля 2006 г. № 149-ФЗ // Собр. законодательства Рос. Федерации – 2006. – № 31, ст. 3448.

7. Форталезская декларация : принята по итогам шестого саммита БРИКС (г. Форталеза, Бразилия, 15 июля 2014 г.). – URL: http:\\www.brics.mid.ru/brics.nsf/WEBdocBric/C9903DE836DEDC0244257D17002A789F.

References

1. Fortalezskaja deklaracija : prinjata po itogam shestogo sammita BRIKS (g. Fortaleza, Brazilija, 15 ijulja 2014 g.). [The Fortaleza Declaration : adopted at the sixth BRICS summit (Fortaleza, Brazil, July 15, 2014)] URL: http:\\www.brics.mid.ru/brics.nsf/WEBdocBric/C9903DE836DEDC0244257D17002A789F.

2. O gosudarstvennoj tajne : zakon RF ot 21 ijulja 1993 g. No. 5485-1 [On State Secrets : Law of the Russian Federation of 21 July 1993 No. 5485-1] // Sobr. zakonodatel'stva Ros. Federacii, 1997. No. 41, art. 8220–8235.

3. O gosudarstvennoj ohrane: federal'nyj zakon RF ot 27 maja 1996 g. No. 57-FZ [On State Guard: the Federal Law of the Russian Federation from May 27, 1996 No. 57-FZ] // Sobr. zakonodatel'stva Ros. Federacii, 1996. No. 22, art. 2594.

4. O svjazi : federal'nyj zakon RF ot 7 ijulja 2003 g. No. 126-FZ [On Signals: the Federal Law of the Russian Federation dated 7 July 2003 No. 126-FZ] // Sobr. zakonodatel'stva Ros. Federacii, 2003. No. 28, art. 2895.

5. Ob informacii, informacionnyh tehnologijah i o zashhite informacii : federal'nyj zakon RF ot 27 ijulja 2006 g. No. 149-FZ [On Information, Information Technologies and Protection of Information : Federal Law of the Russian Federation of July 27, 2006 No. 149-FZ] // Sobr. zakonodatel'stva Ros. Federacii , 2006. No. 31, art. 3448.

6. O personal'nyh dannyh : federal'nyj zakon RF ot 27 ijulja 2006 g. No. 152-FZ [On Personal Data : Federal Law of the Russian Federation of 27 July 2006 No. 152-FZ] // Sobr. zakonodatel'stva Ros. Federacii, 2006. No. 31, art. 3451.

7. O bezopasnosti : federal'nyj zakon RF ot 28 dekabrja 2010 g. No. 390-FZ [On Security : the Federal Law of the Russian Federation of 28 December 2010 No. 390-FZ] // Sobr. zakonodatel'stva Ros. Federacii, 2011. No. 1, art. 2.