УДК 004.056

О.И. Белозеров,
канд. техн. наук, доцент,
доцент кафедры информационных систем и технологий
Хабаровского государственного университета экономики и права
Е.Ю. Сальникова

ОЦЕНКА ЭФФЕКТИВНОСТИ РЕАЛИЗАЦИИ ПОЛОЖЕНИЙ ДОКТРИНЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

В статье ставится задача рассмотреть достоинства и недостатки основных положений Доктрины информационной безопасности Российской Федерации, а также её правовую и материальную основу. Сделан вывод о необходимости пересмотра ряда положений, которые не отвечают реалиям современной жизни.

Ключевые слова: *информационная безопасность, информационная сфера, обеспечение информационной безопасности.*

The article aims to consider the advantages and disadvantages of the basic provisions of the Information Security Doctrine of the Russian Federation, as well as its legal and material basis. It is concluded that it is necessary to revise a number of provisions that do not meet the realities of modern life.

Keywords: *information security, information sphere, provisions of information security.*

За относительно небольшой промежуток времени информационные технологии начали существенно влиять не только на жизнь простых граждан, но и целых государств. В связи с этим информационную политику все чаще называют информационной безопасностью. Какие реальные угрозы несёт интернет-пространство? Какие меры предпринимаются для защиты информационного пространства, информационного суверенитета?

Информационная сфера Российской Федерации является важной частью общественной жизни, во многом определяющей будущие перспективы успешной реализации социально-политических и экономических преобразований российского социума. Главным российским документом, регламентирующим процессы развития общественных отношений и государственной политики в области обеспечения информационной безопасности, является Доктрина информационной безопасности Российской Федерации, утверждённая Указом Президента Российской Федерации 5 декабря 2016 г. (далее – Доктрина) [1].

Данный документ обосновывает объективную необходимость в актуализации правовой основы обеспечения информационной безопасности общества. Как верно отметила М.Ф. Алиева, «информационная безопасность становится важнейшим базовым элементом всей системы безопасности Российского государства» [3]. Настоящая Доктрина является системой официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере. В ней на основе разбора важнейших информационных угроз и оценки состояния информационной безопасности определены стратегиче-

ские цели и основные направления обеспечения информационной безопасности с учетом стратегических национальных приоритетов Российской Федерации [2].

В документе перечисляются основные информационные угрозы. К внешним проявлениям относятся наращивание рядом заграничных государств возможностей информационно-технического влияния на информационную инфраструктуру в военных целях. Одновременно с этим усиливается деятельность разнообразных организаций, осуществляющих техническую разведку в отношении российских органов власти, предприятий оборонно-промышленного комплекса и научных организаций.

К внутренним угрозам относятся: неудовлетворительное состояние отечественных отраслей промышленности и экономики в целом, отставание страны по уровню информатизации органов государственной власти от передовых зарубежных стран, слабая информатизация кредитно-финансовой сферы, промышленности, образования, здравоохранения, сельского хозяйства, сферы услуг и быта граждан. Важный момент – отсутствие исторического, политического и социального опыта жизни в гражданском обществе и правовом государстве, затрудняющее процесс осуществления конституционных прав и свобод граждан, в том числе и в информационной сфере.

Состояние информационной безопасности Российской Федерации показывает, что ее уровень далеко не в полной мере отвечает потребностям общества и государства. Современные условия политического и социально-экономического развития страны вызывают обострение противоречий между нуждами общества в расширении свободного обмена информацией и потребностью сохранения отдельных ограничений. Недостаточная эффективность правового регулирования общественных отношений в информационной сфере приводит к ярко выраженным негативным последствиям. Так, недостаточность нормативного правового регулирования отношений в области реализации конституционных ограничений свободы массовой информации в интересах защиты основ конституционного строя, нравственности, жизни и здоровья, прав и законных интересов граждан, обеспечения обороноспособности страны и безопасности государства значительно способствует затруднению поддержания необходимого равновесия интересов личности, общества и государства в информационной сфере.

Современное состояние нормативно-правового регулирования отношений в сфере массовой информации не препятствует развитию конкурентоспособных средств массовой информации на территории России. Однако необеспеченность прав граждан на свободный доступ к достоверной информации, регулярное манипулирование информацией вызывают ответную негативную реакцию граждан. Таким образом, можно говорить о частичном соблюдении ч. 5 ст. 29 Конституции РФ, в которой гарантируется свобода массовой информации [1].

Закрепленные в Конституции Российской Федерации права граждан на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени (ст. 23) тоже почти не имеют достаточного правового, организационного и технического обеспечения. Неудовлетворительно организована защита персональных данных (данных о физических лицах), собираемых органами государственной власти и местного самоуправления. В качестве яркого примера

можно назвать «Закон Яровой», с вступлением в силу которого на территории Российской Федерации появилась новая обязанность для операторов сотовой связи. Они обязаны хранить записи телефонных сообщений и интернет-трафик их обслуживаемых клиентов.

На первый взгляд принятие такого закона является необходимым условием для противодействия терроризму, обеспечения общественной и государственной безопасности. Однако налицо определенное ущемление конституционных прав и свобод граждан. Вышеупомянутая ст. 23 Конституции гарантирует неприкосновенность частной жизни, что представляет собой запрет на сбор, хранение, распространение информации о жизни человека без его согласия, право на защиту персональных данных [1]. Следовательно, на уровне государства происходит некая нестыковка между провозглашенными ценностями и их реализацией. К недостаткам также можно отнести дополнительные бюджетные расходы, которые должны будут понести операторы сотовой связи на создание такой базы, являющейся платформой для длительного хранения данных пользователей. Получается, что российские IT-компании тратят деньги не на собственное развитие, а на ущемление конституционных прав граждан.

Нет окончательной ясности реализации государственной политики в области защиты российского информационного пространства и его интеграции в мировое информационное сообщество. Данный факт создает предпосылки для искажения структуры международного информационного обмена.

Прогрессирует негативная ситуация с некачественным обеспечением сохранности сведений, составляющих государственную тайну. В результате массового ухода наиболее квалифицированных специалистов нанесен значительный урон кадровому потенциалу научно-производственных коллективов, занимающихся созданием средств информатизации, телекоммуникации и связи.

В Доктрине проводится анализ состояния информационной безопасности в экономической сфере, а также отдельно в области науки, технологий и образования. В связи с этим важно подчеркнуть, что государство впервые поднимает проблему нехватки отечественных технологий, продукции и квалифицированных кадров в информационной сфере до уровня угроз национальной безопасности [6].

Оценивая текущее состояние информационной безопасности в области науки, технологий и образования, разработчики Доктрины делают выпады в адрес российского научного сообщества, указывая на «недостаточную эффективность научных исследований» в соответствующей сфере, «низкий уровень внедрения отечественных разработок».

В целях укрепления информационной безопасности государства от российской науки ожидается существенный вклад в формирование и развитие технологических инноваций. Необходимость в научных знаниях должна учитываться и при совершенствовании законодательства в области информационной безопасности.

В связи с активным проникновением иностранных информационных технологий в сферы деятельности личности, общества и государства, а также с повсеместным использованием открытых информационно-телекоммуникационных систем, их интеграцией с мировыми информационными системами, расширились возможности применения «информационного оружия» против информационной

инфраструктуры Российской Федерации. Работы по комплексному противодействию данным угрозам ведутся при слабой координации и недостаточном бюджетном финансировании. Мало внимания уделяется развитию средств космической разведки и радиоэлектронной борьбы [5].

Указ об утверждении Доктрины вызвал много дискуссий. Часть экспертов недоумевала по поводу ликвидации положений Доктрины 2000 года. Другая часть подвергла документ критике из-за ее ярко выраженной милитаристской направленности. Тем не менее большинство законодателей сошлось во мнении, что принятие Доктрины помогло сфокусировать внимание простых граждан на проблеме. Как известно, гражданская осведомленность является залогом эффективности методов по обеспечению информационной безопасности. Следует отметить, что именно сама российская власть сформировала низкий уровень гражданской осведомленности, забывая о том, что вопрос просвещения граждан крайне важен. До сих пор многие граждане не знают о существовании Доктрины, анализ которой мы проводим. Люди должны быть информированы о возможных рисках и угрозах, должны видеть и распознавать их, применять актуальные технические меры защиты. Основные положения Доктрины информационной безопасности 2000 г. были ориентированы в основном на государственную власть. Документ 2016 г. ориентируется и на обычного человека, в этом заключается принципиальное отличие двух нормативных актов. Кроме того, новая Доктрина учитывает актуальные события и проблемы, например атаки на информационную систему, действия террористических организаций, недостаточную конкуренцию на российском рынке инноваций и многое другое. Учёт существующих проблем и способы их решения являются весомым преимуществом рассматриваемого нормативного акта.

Основным замечанием к Доктрине является её чрезмерно милитаристская направленность. Законодатели слишком усилили заинтересованность в «угрозе, исходящей от стран Запада». При этом борьба с террористическими организациями является второстепенной задачей. Это говорит о векторе развития, направленном в сторону изолированности Российской Федерации от мирового сообщества. Есть мнение, что попытка усилить образ внешнего врага необходима для того, чтобы вытеснить из информационного поля проблемы внутриполитического характера. Безусловно, угроза информационной безопасности России от других государств имеется, отрицать этого нельзя, в то же время информация в Доктрине подается таким образом, что складывается впечатление, будто «одна лишь Россия пытается удержать геополитический баланс и сохранить осуществление и исполнение норм международного права» [5].

Другим весьма важным моментом является тот факт, что с момента принятия Доктрины прошло несколько лет, однако говорить о каких бы то ни было безусловных успехах ее реализации нет особых оснований. По-прежнему остается высокий уровень зависимости отечественной промышленности от зарубежных разработок, по-прежнему российские научные

исследования в области информационных технологий остаются недостаточно эффективными. Обещанной поддержки развития информационных технологий также не наблюдается. Все финансирование государством направляется в несколько крупных центров, например в Сколково, однако отдача от этих вложений далеко не очевидна.

В результате проведённого анализа данной темы можно отметить, что на сегодняшний день российское законодательство не всегда полностью охватывает все аспекты правового регулирования в сфере обеспечения информационной безопасности, часто является устаревшим и не может полностью объективно разрешить имеющиеся проблемы. Следует обозначить острую необходимость ухода от агрессивной риторики как во внутренней, так и во внешней политике. К сожалению, новое законодательство Российской Федерации в данной сфере, например «Закон Яровой», говорит об обратном. Однобокое понимание информационной безопасности ведет Россию к новым шагам в процессе наступления на права и свободы граждан, что в целом создает благодатную почву для дальнейшего роста недоверия между обществом и государством, для усиления кризисных процессов в науке и образовании и технологического отставания во всех наукоемких отраслях.

Список использованных источников

1 Конституция Российской Федерации : принята всенародным голосованием 12.12.1993 г. (в ред. от 21.07.2014 г.) // Собрание законодательства РФ. 2014. № 31. Ст. 4398.

2 Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента РФ от 05.12.2016 г. № 646 // Собрание законодательства РФ. 2016. № 50. Ст. 7074.

3 Алиева М. Ф. Информационная безопасность как элемент информационной культуры / М. Ф. Алиева // Вестник Адыгейского гос. ун-та. 2012. № 4. С. 63–67.

4 Молчанов Н. А. Доктрина информационной безопасности Российской Федерации (новелла законодательства) / Н. А. Молчанов, Е. К. Матевосова // Актуальные проблемы российского права 2017. № 2 (75); https://cyberleninka.ru/article/v/doktrina-informatsionnoy-bezopasnosti-rossiyskoy-federatsii-novella-zakonodatelstva (дата обращения 06.12.2018).

5 Стоякин С. Доктрина информационной безопасности РФ / С. Стоякин // http://fb.ru/article/61751/doktrina-informatsionnoy-bezopasnosti-rossii-osnovnyie-tezisyi (дата обращения 01.06.2019).

6 Васильев Е. Доктрина информационной безопасности 2016 : комплексный подход / Е. Васильев // http://scienceport.ru/anlytics/doktrina-informatsionnoy-bezopasnosti-2016/ (Дата обращения: 12.12.2018).

7 Доктрина информационной безопасности // www.insor-russia.ru/ru/programs/officdoc/1241 (дата обращения 03.06.2019).