ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В РОССИЙСКОЙ ФЕДЕРАЦИИ: ОТДЕЛЬНЫЕ АСПЕКТЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ

https://doi.org/10.33874/2072-9936-2020-0-2-112-117

В настоящее время правовое обеспечение информационной безопасности в Российской Федерации носит фрагментарный характер. Складывается объективная необходимость в совершенствовании действующей нормативно-правовой базы, в разработке и принятии новых правовых документов, которые на современном уровне отвечали бы требованиям по обеспечению информационной безопасности. Все это определяет особую актуальность публикационного материала. В работе подчеркивается, что для решения важнейших вопросов информационной безопасности должны быть задействованы различные отрасли российской правовой системы. Предметом научного исследования являются некоторые аспекты правового регулирования развития информационной безопасности в Российской Федерации. Основная цель работы связана с изучением информационного законодательства и теоретическим осмыслением работ авторов, занимающихся вопросами информационной безопасности, для определения основных направлений информационного обеспечения. Для достижения цели исследования использовалась совокупность философских, общенаучных и частнонаучных методов научного познания. Научная новизна статьи заключается в формировании направлений по совершенствованию правового регулирования информационной безопасности Российской Федерации, что может положительно сказаться на защите государства, общества, гражданина, а также на повышении состояния общего уровня культуры, в том числе и правовой.

СЕРГУН
Петр Павлович

доктор юридических наук, профессор, профессор кафедры административного и муниципального права Саратовской государственной юридической академии (г. Саратов)

sergun-pp@yandex.ru

ГЕРАСИМОВ
Юрий Сергеевич

магистрант Саратовской государственной юридической академии (г. Саратов)

therock09039@gmail.com

Информационная безопасность в Российской Федерации; киберпреступность; информационные угрозы; концепция информационной безопасности; интернет-право; проблемы информационной безопасности; правовая культура

INFORMATION SECURITY IN THE RUSSIAN FEDERATION: SOME ASPECTS OF LEGAL REGULATION

Currently, the legal provision of information security in the Russian Federation is fragmented. There is an objective need to improve the current legal framework, to develop and adopt new legal documents that would meet the requirements for information security at the current level. All this determines the special relevance of the publication material. The paper emphasizes that various branches of the Russian legal system should be involved in solving the most important issues of information security. The subject of scientific research in the article is some aspects of legal regulation of the development of information security in the Russian Federation. The main purpose of the work is to study information legislation and theoretical understanding of the works of authors dealing with information security issues to determine the main directions of information support. To achieve the research goal, a set of philosophical, general scientific and private scientific methods of scientific knowledge was used. The scientific novelty of the article consists in the formation of directions for improving the legal regulation of information security in the Russian Federation, which can have a positive impact on the protection of the state, society, and citizen, as well as on improving the General level of culture, including the legal one.

Peter P. SERGUN

Doctor of Legal Sciences, Professor, Department of Administrative and Municipal Law, Saratov State Law Academy (Saratov)

sergun-pp@yandex.ru

Yuri S. GERASIMOV

Master's Student, Saratov State Law Academy (Saratov)

therock09039@gmail.com

Information security in the Russian Federation; cybercrime; information threats; concept of information security; Internet law; problems of information security; legal culture

В современных условиях происходит усиление информационного противоборства на международном уровне, когда новые *IT*-технологии используются не только в процессе экономической конкуренции между странами, но и для военного противостояния. В этой ситуации особую актуальность приобретает правовое обеспечение информационной безопасности РФ как внутри страны, так и на международной арене. Обеспечение информационной безопасности становится одной из приоритетных задач. Не случайно во всех последних документах, посвященных разработке стратегии национальной безопасности РФ, не только перечисляются основные угрозы, но и определяется совокупность средств, имеющих своей целью обеспечение необходимого уровня информационной защиты нашего государства, общества, гражданина. Эти средства направлены и на формирование общей и правовой культуры.

В нормативно-правовых документах российского законодательства проблеме информационной безопасности страны уделяется определенное внимание. Так, в Стратегии национальной безопасности Российской Федерации 2015 г. в ст. 6 информационная безопасность рассматривается в качестве одной из составляющих национальной безопасности [1]. Доктрина национальной безопасности Российской Федерации 2016 г. также уделяет данному вопросу повышенное внимание: в ст. 26 подчеркивается, что система информационной безопасности является необходимой составляющей системы обеспечения национальной безопасности страны [2].

В настоящее время правовое обеспечение информационной безопасности РФ носит незавершенный характер. Назрела необходимость в разработке и принятии новых нормативно-правовых актов, которые бы на современном уровне обеспечивали информационную безопасность РФ. При этом важен комплексный и системный подход к решению данной проблемы. В этом подходе неоценимую роль могли бы сыграть различные отрасли российского права. Отдельные отрасли права уже себя проявляют. Например, в Уголовном кодексе РФ обеспечению информационной безопасности посвящена гл. 28 «Преступления в сфере компьютерной информации». Однако, как справедливо отмечают специалисты, компьютерная преступность весьма сильно видоизменилась и проникла практически во все сферы жизни российского общества. Это касается не только разглашения банковской, налоговой и коммерческой тайны, но и незаконного проникновения в частную сферу жизни граждан [3, с. 5–6]. А это уже связано с нарушением базовых принципов Конституции РФ.

На основании бурного развития информационных технологий можно прогнозировать дальнейший рост киберпреступности, что приведет к возникновению новых видов преступлений против информационной безопасности РФ. Поэтому действующее гражданское, административное, уголовное законодательство нужно совершенствовать. В этой связи крайне актуальной становится проблема разработки комплексной правовой политики в сфере защиты информационной безопасности РФ.

Концепция государственной информационной политики Российской Федерации предполагает решение следующих основных задач: создание необходимой нормативно-правовой базы для построения информационного общества; всесторонняя подготовка граждан к жизни и работе в современном информационном обществе; развитие независимых средств массовой информации с целью обеспечения граждан достоверной и общественно значимой информацией; обеспечение свободного и широкого доступа к национальным информационным ресурсам на основе их эффективного формирования и использования; развитие современных телекоммуникационных и информационных технологий; постоянная модернизация информационной и телекоммуникационной инфраструктуры [2].

Базовыми принципами государственной информационной политики РФ являются:

1) обеспечение доступа к открытой информации для граждан и организаций;

2) сбор и предоставление информации, которая затрагивает интересы общества;

3) поддержание информационной сферы государства на должном международном уровне.

Данные базовые принципы информационной политики РФ призваны решить такие важные проблемы, как обеспечение информационной прозрачности и гласности в деятельности государства. Это в свою очередь должно способствовать снижению уровня коррупции и злоупотребления властью на местах. Тем самым информационная политика начинает играть приоритетную роль в жизнедеятельности общества. Уже происходят изменения в соотношении ветвей государственной власти. Все бóльшую роль играет информационная власть, которая выходит на приоритетные позиции по сравнению с административной, политической и экономической властями.

Главной целью обеспечения информационной безопасности в стране является создание необходимых экономических, правовых, политических, социальных и культурных условий для эффективного и всестороннего использования различных информационных ресурсов во всех сферах жизни общества.

На наш взгляд, в целях обеспечения информационной безопасности РФ необходимо создать единую систему такого обеспечения, которая бы включала в себя совокупность взаимосвязанных элементов на федеральном, региональном и местном уровнях

управления. Мы разделяем точку зрения К. А. Мамедовой, которая выделяет следующие задачи по обеспечению информационной безопасности в РФ:

во-первых, разработка комплекса продуманных мер по обеспечению информационной безопасности страны на основе учета всех элементов системы управления государственной безопасности;

во-вторых, регулярное и поэтапное формирование информационно-аналитического потенциала страны, призванного осуществлять прогностическую и аналитическую деятельность по предотвращению информационных угроз;

в-третьих, разработка и развитие эффективной системы получения требуемой информации для продвижения стратегических, тактических и оперативных программ по управлению в области информационной безопасности;

в-четвертых, осуществление мер правового характера, связанных с предотвращением противоправной деятельности в сфере обеспечения информационной безопасности страны;

в-пятых, создание механизма по выявлению угроз, возникающих в системе информационной безопасности, что предполагает разработку специального мониторинга состояния информационной безопасности в стране [4, с. 18].

В специальной юридической литературе выделяют три основные группы информационных угроз: угрозы социальным интересам человека, угрозы интересам общества и угрозы интересам государства [5, с. 16].

Наиболее серьезными и опасными источниками информационных угроз для граждан являются: возможности информационного манипулирования сознанием человека за счет включения его в виртуальную реальность; разработка и использование информационных технологий с целью воздействия на психику людей; использование во вред интересам граждан их персональных данных, которые собираются различными информационными структурами, в том числе и государственными; скрытый сбор информации, которая составляет личную и семейную тайну граждан.

Основные информационные опасности для общества представляют собой: все большее усложнение информационно-телекоммуникационных систем, что создает предпосылки для естественных и искусственных сбоев в их работе; увеличение возможностей несанкционированного доступа к информационной инфраструктуре со стороны преступных, экстремистских и террористических организаций; ежегодный рост количества киберпреступлений и потенциала киберпреступности; возможность концентрации массовых средств информации в руках ограниченной группы собственников, которая будет преследовать свои интересы.

Информационные угрозы интересам государства включают в себя: возможности неконтролируемого распространения информационного оружия с целью его использования для достижения неконституционных политических целей; монопольное положение небольшого количества международных компаний на рынке информационных технологий; возможности несанкционированного доступа к сведениям, составляющим государственную тайну; наличие конкурирующих между собой национальных систем информационной безопасности, которые занимаются в том числе и разведывательной деятельностью.

Современный этап правового регулирования информационной безопасности как на международном уровне, так и в РФ характеризуется такой тенденцией, как «суверенизация». Существовавший глобализационный подход, основанный на международно-правовом регулировании информационной безопасности, постепенно сменяется национально-правовым подходом, связанным с внутригосударственным регулированием информационной безопасности страны. Это проявляется, в частности, в создании правовых основ для отказа от выполнения решений международных судов в сфере информационной безопасности.

Как отмечает А. А. Ефремов, изменение федерального законодательства в области правового регулирования информационной безопасности осуществляется по следующим направлениям: 1) вводятся дополнительные требования, связанные с хранением информации организаторами распространения информации в сети Интернет, а также операторами связи; 2) устанавливается порядок ограничения доступа к той информации, которая была обработана с нарушением законодательства РФ в области персональных данных; 3) вводятся ограничения для иностранных лиц, связанные с учреждением средств массовой информации; 4) устанавливается система требований к блогерам и другим организаторам, связанным с распространением информации в сети Интернет; 5) определяется правовой механизм ограничения доступа к той информации, распространение которой запрещено [6, с. 205–206].

В настоящее время в РФ происходит постепенное формирование информационного законодательства, связанного с обеспечением защищенности, устойчивости, стабильности, непрерывности и целостности функционирования национального сегмента сети Интернет. Вместе с тем следует отметить, что отсутствует четкая концептуальная основа для национального информационного суверенитета, а соответствующие законодательные инициативы носят порой разрозненный характер.

С целью усиления правового обеспечения информационной безопасности в РФ можно рекомендовать следующие меры:

во-первых, по делам, связанным с информационной безопасностью, должны быть созданы дополнительные механизмы досудебного и судебного разбирательства, при этом, правоохранительные органы должны иметь, за некоторым исключением, постоянный доступ к информации в Интернете;

во-вторых, должна быть уточнена юридическая ответственность участников информационно-телекоммуникационного процесса; для этого следует обязать авторов отождествлять себя с размещаемой ими информацией;

в-третьих, необходимо более активно развивать международное правовое сотрудничество в сфере информационной безопасности;

в-четвертых, нужно развивать национальный сегмент в Интернете, в частности можно использовать кириллицу для регистрации доменных имен;

в-пятых, необходимо оказывать содействие на правовом уровне участникам виртуального общения.

Следует согласиться с позицией Ю. В. Слесарева и А. В. Лосякова, которые предлагают следующие меры по обеспечению информационной безопасности в РФ:

– четкое определение того круга лиц, которые наделены правом работы с информацией ограниченного доступа;

– ужесточение законодательства по отношению к лицам, работающим с конфиденциальной информацией, за халатное отношение к своим обязанностям;

– необходимость создания единого международного правового пространства в целях обеспечения информационной безопасности;

– введение дополнительных нормативно-правовых актов, которые касаются распространения в интернете информации о частной жизни граждан;

– законодательное разграничение и строгое соблюдение иерархии конфиденциальной информации с нужной степенью правовой защиты [7, с. 384].

Одним из основных направлений обеспечения информационной безопасности в РФ является противодействие экстремизму и терроризму в Интернете. Перед российским законодательством стоит важная и сложная задача совершенствования правовой основы борьбы с правонарушениями, связанными с проявлением экстремизма в сети Интернет. В настоящее время существует неослабевающая угроза распространения экстремизма и терроризма в первую очередь через глобальные сети.

Совершенствование правовой основы борьбы с правонарушениями, связанными с проявлением экстремизма в сети Интернет, предполагает поиск баланса между защитой прав и свобод граждан от проявлений экстремизма и терроризма и нарушением этих же прав со стороны государства в процессе его борьбы с экстремистской и террористической деятельностью. В формировании такого баланса особую роль должны играть законодательные и судебные органы.

Отсутствие полной ясности с использованием понятий «экстремизм», «экстремистская деятельность в сети Интернет» препятствует реализации и защите прав и свобод граждан. Поэтому совершенствование правовой основы борьбы с правонарушениями, связанными с проявлением экстремизма в сети Интернет, предполагает также уточнение и корректное использование соответствующих базовых понятий.

Как справедливо отмечают М. А. Лапина и В. С. Николаенко, благодаря необходимости административно-правового регулирования информационной сферы в РФ возникло специфическое направление в деятельности государства – информационная функция государства [8, с. 12]. Носителем данной функции стал специальный государственный орган – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Данный орган исполнительной власти в соответствие с законодательством РФ наделен специальными полномочиями по надзору за деятельностью тех субъектов, которые занимаются организацией по распространению информации в телекоммуникационных сетях. Роскомнадзор осуществляет следующие направления деятельности:

во-первых, предоставление уведомления о начале осуществления деятельности, связанной с функционированием информационных систем и вычислительных машин, которые предназначены для использования в сети Интернет;

во-вторых, надзор и контроль за деятельностью тех субъектов, которые организуют процесс распространения информации в телекоммуникационных сетях (речь идет о хранении, передаче и использовании письменных, голосовых, изобразительных и других сообщений в сети Интернет);

в-третьих, контроль за предоставлением органам Роскомнадзора обязательного экземпляра электронного издания [9].

В настоящее время важной и до конца не решенной проблемой остается создание целостной концепции интернет-права, которая охватывала бы все основные направления и аспекты административно-правового функционирования телекоммуникационных и информационных систем. Данная концепция, как отмечает И. М. Рассолов, должна не только основываться на информационном праве, но и взаимодействовать с международным публичным правом, международным частным правом, гражданским правом, уголовным правом [10].

Одной из трудностей, которая препятствует формированию современной административно-правовой

концепции обеспечения информационной безопасности в РФ, является отсутствие четкого юридического определения понятия «Интернет». В информационном праве до настоящего времени используется преимущественно техническое определение данного понятия. Этого явно недостаточно для его применения в сфере различных правовых отношений.

А. С. Маякова и С. А. Шелепова справедливо отмечают, что в Уголовном кодексе РФ не закреплено понятие «компьютерное преступление». Данную категорию обычно относят к криминологическим понятиям. Компьютерной преступностью (киберпреступностью) в специальной литературе принято называть совокупность таких преступных деяний, которые имеют предметом своих посягательств компьютерную информацию [11, с. 192]. На наш взгляд, следовало бы закрепить в российском законодательстве понятия «компьютерное преступление», «компьютерное правонарушение». Такой подход позволил бы повысить правовую культуру в вопросах правоприменения и защиты государства, общества, гражданина в сфере информационной безопасности.

Исходя из изложенного можно сделать следующие выводы:

1. Понятие «информационная безопасность» характеризуется многоаспектностью, что предполагает использование комплексного подхода к анализу понятия и базовых принципов информационной безопасности в РФ.

2. Цели обеспечения информационной безопасности находятся в системном единстве с источниками информационных опасностей в РФ. Необходимо постоянно корректировать данные цели в зависимости от модификации источников информационных опасностей.

3. Система информационной безопасности находится в комплексном единстве с доктриной национальной безопасности России. Необходимо реализовывать конкретно-исторический подход к концепциям информационной безопасности и национальной безопасности РФ.

4. Научный системный подход должен быть применен и к основным направлениям обеспечения информационной безопасности в РФ. Ключевые тенденции в развитии информационной безопасности связаны с процессами экономической глобализации и с построением информационного общества. В этой связи особую актуальность приобретает современное правовое регулирование информационной безопасности России.

5. Теоретический подход к анализу предупредительно-карательных методов обеспечения информационной безопасности должен исходить из совокупности гражданского, административного, уголовного законодательства по регулированию вопросов обеспечения информационной безопасности в РФ.

Пристатейный библиографический список

1. Указ Президента РФ от 31 декабря 2015 г. № 683 «О стратегии национальной безопасности Российской Федерации» // СЗ РФ. 2016. № 1. Ст. 212.

2. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. № 50. Ст. 7074.

3. *Ефремова М. А.* Уголовно-правовая охрана информационной безопасности : дис. … докт. юрид. наук. М., 2017.

4. *Мамедова К. А.* Основные принципы обеспечения информационной безопасности страны // Информационная безопасность регионов. 2016. № 1 (22).

5. *Егоров В. А.* Классификация источников угроз безопасности информационного общества // Информационная безопасность регионов. 2009. № 1 (4).

6. *Ефремов А. А.* Формирование концепции информационного суверенитета государства // Право. Журнал Высшей школы экономики. 2017. № 1.

7. *Слесарев Ю. В., Лосяков А. В.* Проблемы защиты конфиденциальной информации в сети Интернет : правовой аспект // Балтийский гуманитарный журнал. 2018. Т. 7. № 1 (22).

8. *Лапина М. А., Николаенко В. С.* Информационная функция государства в сети Интернет // Информационное право. 2013. № 4.

9. *Бачило И. Л.* Информационное право : учебник для академического бакалавриата. М. : Юрайт. 2016.

10. *Рассолов И. М.* Информационное право : учебник для магистров. М. : Юрайт, 2013.

11. *Маякова А. С., Шелепова С. А.* Компьютерные преступления : отдельные вопросы квалификации // Проблемы экономики и юридической практики. 2017. № 6.

References

1. Decree of the President of the Russian Federation of 31 December 2015 No. 683 "On the Strategy of National Security of the Russian Federation". *Collection of the Legislation of the Russian Federation*. 2016. No. 1. Art. 212.

2. Decree of the President of the Russian Federation of 5 December 2016 No. 646 "On Approval of the Doctrine of Information Security of the Russian Federation". *Collection of the Legislation of the Russian Federation*. 2016. No. 50. Art. 7074.

3. *Ephraim M. A.* Criminal-Legal Protection of Information Security: Thesis for a Doctor Degree in Law Sciences. Moscow, 2017.

4. *Mamedova K. A.* Basic Principles of Ensuring Information Security of the Country. *Information Security of Regions*. 2016. No. 1 (22).

5. *Egorov V. A.* Classification of Sources of Threats to the Security of Information Society. *Information Security of Regions*. 2009. No. 1 (4).

6. *Efremov A. A.* Formation of the Concept of Information Sovereignty of the State. *Law. Journal of the Higher School of Economics*. 2017. No. 1.

7. *Slesarev Iu. V., Losiakov A. V.* Problems of Protecting Confidential Information on the Internet: A Legal Aspect. *Baltic Humanitarian Journal*. 2018. Vol. 7. No. 1 (22).

8. *Lapina M. A., Nikolaenko V. S.* Information Function of the State in the Internet. *Information Law*. 2013. No. 4.

9. *Bachilo I. L.* Information Law: Textbook for Academic Bachelor's Degree. Moscow: Iurait, 2016.

10. *Rassolov I. M.* Information Law: Textbook for Masters. Moscow: Iurait, 2013.

11. *Maiakova, S. A., Shelepova S. A.* Cybercrime: Selected Issues of Qualification. *Problems of Economics and Legal Practice*. 2017. No. 6.