

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Мысев А.Э.¹, Морозов Н.В.²

¹Мысев Алексей Эдуардович - магистрант,

кафедра общей юриспруденции и правовых основ безопасности;

²Морозов Николай Владимирович – кандидат юридических наук, доцент,

отделение интеллектуальных кибернетических систем офиса образовательных программ,
Национальный исследовательский ядерный университет МИФИ,
г. Москва

Аннотация: законодательство в сфере информационной безопасности является сравнительно молодой отраслью законодательства не только в Российской Федерации, но и в мире. Стремительное развитие информационных технологий, сети «Интернет» и общественных отношений в информационной сфере привело различные государства к необходимости урегулирования, в том числе и правовой политики в отношении информационной безопасности. В Российской Федерации информационная безопасность рассматривается как одна из составляющих национальной безопасности государства. В данной работе рассматриваются основные нормативно-правовые акты в сфере информационной безопасности, а также Доктрина информационной безопасности Российской Федерации. Проводится сравнительный анализ положений Доктрины 2000 года и Доктрины 2016 года. В рамках анализа изменений также рассматриваются угрозы информационной безопасности Российской Федерации, а также текущие результаты по регулированию таких угроз.

Ключевые слова: информация, информационная безопасность, национальная безопасность, компьютерная преступность, защита информации, импортозамещение, система управления информационной безопасностью, информационная сфера.

Введение

История информационной безопасности начинается задолго до XX века, однако в современной трактовке [1] понятие «информационная безопасность» как и сам термин «информация» в большинстве случаев неразрывно связано именно с применением компьютерных технологий в связи со стремительным развитием данной сферы во второй половине XX века, которое продолжается и на сегодняшний день.

В Российской Федерации (далее – РФ) с 1995 г. по 2006 г. основополагающим законодательным актом, регулирующим общественные отношения в информационной сфере, являлся Федеральный закон РФ «Об информации, информатизации и защите информации» [2], правовую основу которого составляла Конституция РФ 1993 г. [3]. Основные положения Закона включали в себя регулирование общественных отношений в вопросах формирования и использования информационных ресурсов, создание и использовании информационных технологий, защиты информации и др. (ст.1, п.1). При этом обеспечение национальной безопасности в сфере информатизации было определено как одно из основных направлений государственной политики в сфере информатизации (ст.3, п.2).

Федеральный закон РФ «Об информации, информатизации и защите информации» был отменен в 2006 г. в связи с принятием в том же году Федерального закона РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» [4], который существенно дополнил правовую базу отмененного закона и до сих пор остается основополагающим нормативным правовым актом в информационной сфере.

В дополнении к рассмотренным Федеральным законам была также утверждена Доктрина информационной безопасности РФ 2000 г. [5], которая утратила силу в связи с утверждением указом Президента РФ новой Доктрины информационной безопасности РФ 2016 г. [1]. Настоящая Доктрина в совокупности с Федеральными законами, другими нормативными правовыми актами РФ и федеральных органов исполнительной власти, указами Президента РФ и постановлениями Правительства РФ составляет правовую основу в сфере информационной безопасности.

Сравнительный анализ положений Доктрин информационной безопасности РФ.

Согласно Доктрине 2000 г. [5] данный документ развивал Концепцию национальной безопасности РФ применительно к информационной сфере, в то время как Доктрина 2016 г. [1] является документом стратегического планирования в сфере обеспечения национальной безопасности РФ, в котором развиваются положения Стратегии национальной безопасности РФ [6], утвержденной Указом Президента РФ от 31.12.2015 № 683, а также других документов стратегического планирования в указанной сфере.

В отличие от Доктрины 2000 г. в новой Доктрине однозначно закреплены основные понятия и термины, используемые в документе, в том числе и ранее неопределенные, что снижает вероятность

неверной интерпретации используемой терминологии. Также все понятия были вынесены в отдельный пункт документа (разд. I, п.2) и значительно расширено понятие информационной безопасности.

Как отмечается в [7] в новой Доктрине текущее состояние информационной безопасности и направления обеспечения информационной безопасности рассматриваются в разрезе стратегических национальных приоритетов, обозначенных в новой Стратегии национальной безопасности РФ. Благодаря этому документ является более структурированным и последовательным относительно версии 2000 года.

Таким образом, новая Доктрина информационной безопасности РФ не только является логическим продолжением Стратегии национальной безопасности РФ по своей направленности, но и по структуре, что должно в перспективе позволить выстраивать всю иерархию документов в сфере информационной безопасности с учетом соответствующих стратегических национальных приоритетов [7].

Стоит отметить тот факт, что в Доктрине 2000 г. уделяют внимание вопросу роста влияния информационных технологий на национальные интересы государства, что же касается Доктрины 2016 г., то сфера информационных технологий рассматривается как непосредственная часть жизни общества.

Что касается положений новой Доктрины, то они отвечают современным тенденциям, как в области информационной безопасности, так и в сфере информационных технологий.

Следует обратить внимание на то, что в новой Доктрине сформированы положения Стратегии национальной безопасности РФ, которые касаются:

- усиливающегося противоборства в мировом информационном пространстве;
- угроз нарушения безопасности и устойчивости функционирования критической информационной инфраструктуры РФ;
- деятельности, которая связана с использованием информационных и коммуникационных технологий в экстремистской деятельности;
- импортозамещения и уменьшения критической зависимости от иностранных технологий и промышленной продукции.

Курс на импортозамещение четко прослеживается в обеих версиях документов. Тем не менее, следует отметить, что в новой Доктрине экономическая сфера обеспечения информационной безопасности сосредоточена именно на важности и необходимости формирования отрасли информационных технологий и информационной безопасности.

Новый документ призывает к ликвидации какой-либо зависимости от зарубежных информационных технологий, что является частью стратегии информационной безопасности РФ.

В новой Доктрине говорится о том, что одним из наиболее важных направлений развития информационной безопасности государства является создание благоприятных условий для создания и развития технологических компаний на территории Российской Федерации.

Как отмечается в [7] Еще одним не менее важным нововведением Доктрины информационной безопасности РФ 2016 года являются усовершенствованные задачи государственных органов в рамках деятельности по формированию и усовершенствованию системы обеспечения информационной безопасности, а именно:

- укрепление вертикали управления и централизация сил обеспечения информационной безопасности на федеральном, межрегиональном, региональном, муниципальном уровнях, а также на уровне объектов информатизации, операторов информационных систем и сетей связи;
- совершенствование форм и методов взаимодействия сил обеспечения информационной безопасности в целях повышения их готовности к противодействию информационным угрозам, в том числе путем регулярного проведения тренировок (учений);
- совершенствование информационно-аналитических и научно-технических аспектов функционирования системы обеспечения информационной безопасности;
- повышение эффективности взаимодействия государственных органов, органов местного самоуправления, организаций и граждан при решении задач по обеспечению информационной безопасности[7].

В связи с тем, что происходит непрерывное увеличение угроз информационной безопасности, в новой Доктрине уделяется внимание такому вопросу, как защита критической информационной инфраструктуры, делается упор на то, что важно обеспечивать бесперебойное и устойчивое функционирование данной инфраструктуры РФ. Стоит отметить, что в предыдущей версии Доктрины данной проблеме не было уделено положенного внимания.

В документе уделяется пристальное внимание такому вопросу, как защита частной жизни граждан вследствие обработки персональных данных с помощью современных информационных технологий. Согласно новой Доктрине одним из наиболее важных аспектов защиты частной жизни гражданина должна стать эффективная защита информационных систем и прочих объектов, которые тем или иным способом задействованы в обработке персональных данных.

Стоит обратить внимание на то, что в целях улучшения состояния информационной безопасности реализуется развитие и совершенствование национальной системы управления российским

сегментом сети «Интернет». Следует отметить, что количество внешних угроз, которые неблагоприятно влияют на информационную безопасность страны, к сожалению, возрастает. Тем самым происходит усугубление проблем, которые напрямую связаны с блокированием деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории. В связи с этим взгляды на необходимость поддерживать и укреплять государственные СМИ, доводящие до российской и международной общественности достоверную информацию о государственной политике Российской Федерации, также не изменились [7].

Резюмируя вышесказанное, новая Доктрина информационной безопасности РФ продолжает курс, который был задан предыдущей версией документа, но при этом учитываются изменения, которые происходят в сфере информационных технологий.

Реализация стратегий борьбы с угрозами, определенными в положениях новой Доктрины РФ

В рамках разработки новой Доктрины были актуализированы угрозы информационной безопасности РФ (разд. III, п. 10-19). Ниже представлены наиболее важные успехи в преодолении этих угроз на текущий момент.

Для разрешения вопроса противодействия компьютерным атакам (разд. III, п. 16) в 2017 г. был представлен, а впоследствии принят Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной структуры Российской Федерации» [8]. Данный закон на текущий момент является одним из прямых примеров реализации стратегии, описанной в новой Доктрине.

В новой Доктрине в качестве информационной угрозы также отмечается участвовавшее негативное воздействие зарубежными системами массовой информации на граждан РФ в виде недостоверных материалов (разд. III, п. 12). В противодействие этому МИД РФ в 2017 г. Запустил проект по опровержению данных материалов, на момент написания настоящей статьи число таких опровержений равно 47. Хотя противодействие данной угрозе носит скорее информационный характер, непосредственно полное исключение угрозы на текущем этапе развития мировой информационной сферы представляется маловероятным.

Дополнительно, для разрешения вопроса достоверности материалов в сети «Интернет» были принят Федеральный закон от 29.07.2017 № 276-ФЗ «О внесении изменений в Федеральный закон “Об информации, информационных технологиях и о защите информации”» [9], в котором были отражены важнейшие изменения касательно информационно-телекоммуникационных сетей и информационным ресурсам посредством которых осуществляется доступ к таким же сетям и ресурсам, доступ к которым уже ограничен на территории РФ.

Выводы

В конце 2016 г. была утверждена новая Доктрина информационной безопасности РФ, обновленная с учетом современного состояния информационной сферы в РФ и положения РФ в мировом информационном сообществе. Доктрина точно отражает стратегию развития РФ в области информационной безопасности на ближайшее будущее и является несомненным улучшением по сравнению с предыдущей версией Доктрины 2000 г. В рамках обеспечения выполнения данной стратегии в законодательстве РФ на текущий момент разработаны нормативно-правовые акты, адресующие решения для части важных для устранения угроз, описанных в Доктрине. Тем не менее, остается еще ряд угроз, решения для которых в ближайшее время будет найти затруднительно. В случае разрешения вопроса о продвижения концепции Конвенции о международной информационной безопасности, разработанной в РФ, на международной арене, вероятнее всего удастся разработать решения для той части угроз, что невозможно полностью устранить силами одного государства, но для этого должны быть заинтересованы и другие страны-участники. В рамках внутренней политики также остается немало существующих проблем, для устранения которых также требуется разработать качественную нормативную базу, обеспечивающую защиту личности, общества и государства от внешних и внутренних информационных угроз.

Список литературы

1. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 5 декабря 2016 г. № 606).
2. Федеральный закон РФ «Об информации, информатизации и защите информации» от 27 июля 2006 г. № 149 - ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 14 июля 2006 г. // Российская газета – 2006. – 29 июля.
3. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ).
4. Федеральный закон РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации».

5. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. № Пр-1895) (утратила силу).
6. Указ Президента Российской Федерации от 31 декабря 2015 года № 683 «О Стратегии национальной безопасности Российской Федерации»
7. А.Мещерякова «Сравнение Доктрин ИБ РФ 2000 года и 2016 года» // НвсФ ФГУП «НТЦ «Атлас» - [Электронный ресурс] – Режим доступа: <https://www.atlas-nsk.ru/news/186/> (дата обращения: 20.05.2019).
8. Федеральный закон РФ «О безопасности критической информационной структуры» от 26 июля 2017 г. № 187 - ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 12 июля 2017 г. // Российская газета – 2017. – 31 июля.
9. О внесении изменений в статьи 10.4 и 15.3 Федерального закона «Об информации, информационных технологиях и о защите информации» и статью 6 Закона Российской Федерации «О средствах массовой информации»: федеральный закон от 25 ноября 2017 г. N 327 - ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 15 ноября 2017 г. // Российская газета – 2017. – 27 ноября.