

УДК 316.77(470+571)

ТУМАНОВА ОЛЬГА ИГОРЕВНА

АНАЛИЗ ОТДЕЛЬНЫХ ПОЛОЖЕНИЙ «ДОКТРИНЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ»

АННОТАЦИЯ

В статье представлен анализ отдельных положений Доктрины информационной безопасности Российской Федерации.

Ключевые слова: национальная безопасность; национальные интересы; информационная безопасность; доктрина.

TUMANOVA O.I.

ANALYSIS OF SEPARATE ASPECTS OF "INFORMATION SECURITY DOCTRINE OF THE RUSSIAN FEDERATION"

ABSTRACT

The article presents an analysis of some items of the Doctrine of Information Security of the Russian Federation.

Keywords: national security; national interests; information security; doctrine.

Вызовы в информационной сфере, наряду с террористической и экстремистской деятельностью на сегодняшний день входят в число самых серьезных угроз национальной безопасности государства. Глобальность и стремительное развитие информационной среды требуют создания полноценной системы защиты интересов страны и граждан. При этом следует учитывать, что обеспечение информационной безопасности должно являться комплексным элементом общей системы государственной безопасности.

Одним из значимых событий в процессе формирования системы информационной безопасности является подписание Президентом в конце 2016 года Доктрины информационной безопасности Российской Федерации (Указ Президента РФ от 5 декабря 2016 г. № 646) (далее – Доктрина). Новая трактовка Доктрины разра-

ботана с учетом изменений произошедших внутри страны и во внешнеполитической сфере и является ответом на возникающие и расширяющиеся списки угроз национальным интересам в сфере использования, распространения, передачи и защиты информации.

В отличие от предыдущей версии документа, (утвержденной Президентом РФ от 9 сентября 2000 г. N Пр-1895) новая Доктрина носит системный характер. В частности, при сравнении преамбул документ 2000-го года охарактеризован как совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации [1]. В тексте 2016 года Доктрина определена уже как система официальных взглядов на обеспечение национальной безопасности [2].

В новом документе можно выделить ряд принципиальных моментов, которые позволяют расставить акценты в деятельности по обеспечению информационной безопасности государства.

В первую очередь следует отметить, что в Доктрине четко обозначен перечень национальных интересов в информационной сфере. К ним относятся:

а) обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий, обеспечение информационной поддержки демократических институтов, механизмов взаимодействия государства и гражданского общества, а также применение информационных технологий в интересах сохранения культурных, исторических и духовно-нравственных ценностей многонационального народа Российской Федерации;

б) обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура) и единой сети электросвязи Российской Федерации, в мирное время, в период непосредственной угрозы агрессии и в военное время;

в) развитие в Российской Федерации отрасли информационных технологий и электронной промышленности, а также совершенствование деятельности производственных, научных и научно-технических организаций по разработке, производству и эксплуатации средств обеспечения информационной безопасности, оказанию услуг в области обеспечения информационной безопасности;

г) доведение до российской и международной общественности достоверной информации о государственной политике Российской Федерации и ее официальной позиции по социально значимым событиям в стране и мире, применение информационных технологий в целях обеспечения национальной безопасности Российской Федерации в области культуры;

д) содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности, на укрепление равноправного стратегического партнерства в области информационной безопасности, а также на защиту суверенитета Российской Федерации в информационном пространстве [2].

Очевидно, что перечисленные национальные интересы касаются не только внутренней жизни государства и его граждан, но и касаются функционирования информационного пространства в международном масштабе. Кроме этого, документ затрагивает процессы развития и функционирования информационной инфраструктуры.

Важным моментом является характеристика общего состояния информационной безопасности в государстве и четкое определение в документе основных информационных угроз, в числе которых отмечают:

- наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях,
- усиление деятельности организаций, осуществляющих техническую разведку в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса;
- расширяются масштабы использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира;
- отмечается тенденция к увеличению в зарубежных средствах массовой информации объема материалов, содержащих предвзятую оценку государственной политики Российской Федерации;
- наращивается информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей;

- террористическими и экстремистскими организациями создаются средства деструктивного воздействия на объекты критической информационной инфраструктуры;
- возрастают масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере;
- увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий [2].

Рассмотренные в документе угрозы в информационной сфере нашли свое отражение и в выступлении Президента Российской Федерации Владимира Путина 16 февраля 2017 года, на ежегодном расширенном заседании коллегии ФСБ, посвященном итогам деятельности ведомства за прошедший период и приоритетным задачам в области обеспечения национальной безопасности. Президент в частности обозначил ряд актуальных направлений в деятельности спецслужб, в числе которых работа по совершенствованию системы защиты сведений, составляющих государственную тайну, особенно в условиях перехода ведомств на электронный документооборот [3]. Было отмечено также увеличение в три раза количества компьютерных атак на официальные государственные информресурсы в 2016 году, по сравнению с предыдущим годом. В связи с этим была обозначена необходимость развития ведомственных сегментов Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы [3].

Доктрина устанавливает основные направления обеспечения национальной безопасности. Это обороны страны, экономическая сфера, область науки, технологий и образования, область стратегической стабильности и равноправного стратегического партнерства [2]. Данные направления совпадают с основными стратегическими национальными приоритетами, закрепленными в Стратегии национальной

безопасности. Подобная взаимосвязанность свидетельствует о том, что новая Доктрина вошла в число основополагающих документов регламентирующих систему защиты национальных интересов и национальной безопасности. При этом система обеспечения информационной безопасности определена как часть системы национальной безопасности [2].

Доктрина намечает организационные основы обеспечения национальной безопасности в информационном поле. В частности в документе определены организационные основы системы обеспечения информационной безопасности; сформулированы задачи государственных органов в рамках деятельности по обеспечению информационной безопасности, сформулированы задачи государственных органов в рамках деятельности по развитию и совершенствованию системы обеспечения информационной безопасности.

В новом тексте Доктрина определены основные принципы, на которых основывается деятельность государственных органов по обеспечению информационной безопасности. В условиях сложной внешнеполитической обстановки особенно важным представляется выделение принципа соблюдения общепризнанных принципов и норм международного права, международных договоров Российской Федерации, а также законодательства Российской Федерации [2]. Именно Российская Федерация на сегодняшний день вносит решающий вклад в сохранении системы международного права, подчеркивая ее авторитетность и незыблемость, в том числе и в международном информационном пространстве.

Усилия России по защите информационного пространства подчеркивает секретарь Совета Безопасности Российской Федерации Николай Патрушев, говоря о том, что «на международной арене стратегической целью России является формирование такой системы, которая базировалась бы на общепризнанных правилах ответственного поведения государств в информационном пространстве. Соответствующая работа последовательно проводится в рамках Группы правительственных экспертов ООН. Наглядным свидетельством востребованности

такого курса служит принятая Генассамблеей по инициативе России резолюция «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» [4].

В числе прочих в Доктрине выделяется принцип декларирующий соблюдение баланса между потребностью граждан в свободном обмене информацией и ограничениями, связанными с необходимостью обеспечения национальной безопасности, в том числе в информационной сфере [2]. Важно, что разработчики документа определяют и фиксируют тонкую грань между свободным обменом и распространением информации и контролем и цензурой в информационном поле. Наличие этой грани ярко показало активное общественно-политическое обсуждение антитеррористического пакета законов (т.н. «пакет Яровой»), затронувших информационную сферу.

Подводя итоги, следует отметить, что появление Доктрины как программного документа способно не только определить основные направления деятельности, но и создать прочную основу для дальнейшего формирования нормативно-правовой базы для защиты национальных интересов в информационной сфере.

Кроме этого, можно говорить о том, что рассматриваемый документ задает определенный вектор развития для всех участников системы обеспечения информационной безопасности. Дальнейшая работа должна проводиться в условиях согласованности и взаимодействия для формирования комплекса мер по защите информационного пространства.

Например, в качестве одного из элементов системы обеспечения информационной безопасности можно рассматривать создание Министерством Обороны Российской Федерации войск информационных операций. Это формирования российской армии, основными задачами которого являются управление и защита военных компьютерных сетей, защита российских военных систем управления и связи от кибератак и надежное прикрытие проходящей по ним информации. «Информационные войска» осуществляют координацию и интеграцию операций,

проводимых киберподразделениями, экспертизу кибернетического потенциала Минобороны России и расширяют возможности его действий в кибернетическом пространстве [5].

Подобные действия свидетельствуют о том, что параллельно разработке программных документов уже ведется практическая работа, позволяющая формировать полноценную систему защиты национальных интересов в информационном пространстве. Наличие и постоянное развитие такой системы позволит своевременно отвечать на вызовы и защищать интересы граждан и государства в информационной сфере.

Список литературы

1. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. N Пр-1895) [Электронный ресурс]. – Режим доступа: <http://base.garant.ru/182535/> (дата обращения 19.03.2017).
2. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс]. – Режим доступа: <http://publication.pravo.gov.ru/Document/View/0001201612060002> (дата обращения 19.03.2017).
3. Владимир Путин принял участие в ежегодном расширенном заседании коллегии ФСБ, посвященном итогам деятельности ведомства за прошедший период и приоритетным задачам в области обеспечения национальной безопасности [Электронный ресурс]. – Режим доступа: <http://nac.gov.ru/hronika-sobytyi/vladimir-putin-prinyal-uchastie-v-ezhegodnom-rasshirennom.html> (дата обращения 19.03.2017).
4. Николай Патрушев. Мир без иллюзий и мифов [Электронный ресурс]. – Режим доступа: <https://rg.ru/2017/01/15/patrushev-illuzij-o-skorom-oslablenii-mer-sderzhivaniia-rossii-nepitaem.html> (дата обращения 19.03.2017).
5. Шойгу объявил о создании войск информационных операций [Электронный ресурс]. – Режим доступа: <https://rg.ru/2017/02/22/shojgu-obiavil-o-sozdanii-vojsk-informacionnyh-operacij.html> (дата обращения 19.03.2017).