

Галушкин Александр Александрович,
*кафедра судебной власти, правоохранительной
и правозащитной деятельности
Российский университет дружбы народов
alexander.galushkin@yandex.ru*

НАЦИОНАЛЬНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В УСЛОВИЯХ ГЛОБАЛИЗАЦИИ

В настоящей статье автором обосновывается необходимость комплексного подхода к обеспечению информационной безопасности в границах государства (на национальном уровне), создания специализированной нормативно-правовой базы, отвечающей современным условиям глобализации, а также целесообразность создания специализированных служб.

Ключевые слова и фразы: информация, информатизация, защита информации, государство, право, общество, глобализация.

В контексте защиты информации и обеспечения режима информационной безопасности особый интерес представляют следующие этапы научно-технической революции:

- изобретение письменности, в результате чего стала возможной передача информации на материальном носителе;
- изобретение книгопечатания – после этого стало возможным более или менее массовое тиражирование рукописей;

¹ <http://www.imf.org/external/pubs/ft/aa/rus/index.pdf>

- изобретение телеграфа и телефона открыло возможность для быстрой передачи информации на большие расстояния;
- изобретение компьютеров, информационно-телекоммуникационной сети Интернет (далее – Интернет) и их повсеместное облегчило передачу больших объемов информации внутри глобальной международной сети.

Безусловно, вопросы защиты информации были актуальны во все времена и эпохи. С развитием науки и техники появлялись новые способы передачи и хранения информации, и, соответственно, способы защиты информации.

В XXI веке информационные технологии сыграли особо важную роль. Уже недостаточно просто обеспечить безопасность на отдельно взятом объекте: будь то предприятие, учреждение или организация, вне зависимости от их организационно-правовой формы и направлений деятельности. Все более актуальными стали вопросы комплексного обеспечения информационной безопасности как на государственном (национальном), так и на международном (транснациональном) уровне.

Многочисленные хакерские атаки и диверсионно-террористические операции, проведенные с использованием новейших информационных технологий и специального программного обеспечения через сеть Интернет, а также различных внутренних сетей, имеющих выход в Интернет показали, что обеспечение информационной безопасности на уровне конкретного объекта, имеющего внешний выход в сети общего доступа или удаленный доступ, весьма проблематично и подчас неэффективно.

Полноценное обеспечение информационной безопасности на государственном (национальном) уровне становится в современных условиях основой не только безопасности отдельных государственных, муниципальных или частных объектов, но и государства в целом. Во многих развитых странах уже давно созданы специальные правоохранительные службы или специализированные подразделения, активно занимающиеся вопросами обеспечения информационной безопасности на государственном уровне (национальной информационной безопасности). Обычно дополнительно создаются научные и научно-исследовательские институты и центры, специализирующиеся на разработке новых методов, технологий, оборудования, способного эффективнее выявлять

возможные угрозы, фиксировать их, по возможности противодействовать им, а также подводить необходимые статистические данные, таким образом посильно участвуя в обеспечении информационной безопасности как на национальном (государственном) уровне, так и на локальном (здание, объект, предприятие, организация или учреждение) уровне.

Российская Федерация относительно недавно окунулась в проблемы информационной безопасности, в силу ряда объективных причин.

В конце XX века в нашей стране произошли существенные перемены в социальной, экономической, общественной сферах. Распад Советского Союза привел к множественным изменениям в гражданском обществе. Появились иностранные товары, технологии и услуги, многие из которых вообще не были ранее представлены в СССР или круг лиц, пользовавшихся таковыми в эпоху существования Советского Союза, существенно ограничен. Не исключением стали и информационные, в том числе телекоммуникационные технологии. Так появились и получили широкое распространение персональные компьютеры (электронные вычислительные машины) и иностранное программное обеспечение к ним, а также принтеры, сканеры, и другое сопутствующее оборудование как гражданского, так и военного, а также двойного назначения.

Российская Федерация, в отличие от других государств мира, почувствовала результаты четвертой информационной революции, связанной с изобретением и внедрением в массовое производство микропроцессоров и их специализированное программирование, а также появление персональных переносных компьютеров и технологий передачи информации (в том числе протоколов). Внедрение после распада СССР данных технологий в массовое использование, в том числе открытие для массового пользователя доступа к международной информационно-телекоммуникационной сети Интернет, и расширения доступа в сетях типа интранет.

Внедрение новых технологий породило и новые проблемы. С внедрением информационных технологий, активной компьютеризацией и переводом данных в электронную форму хранения появилась необходимость защиты информации, хранящейся на электронных (в том числе сетевых) носителях.

В современном мире информационная безопасность государства по своей сути является составной частью его национальной безопасности и выражается в комплексе организационно-правовых инструментов по обеспечению сохранности важной для государства информации, организации соответствующего режима доступа к ней, воспрепятствованию её несанкционированного удаления и изменения, обеспечения защищённости законных прав и свобод человека и гражданина.

В свете вышеизложенного интересен п. 109 Стратегии национальной безопасности Российской Федерации до 2020 года, утвержденной Указом Президента Российской Федерации от 12.05.2009 № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года», который гласит, что «угрозы информационной безопасности в ходе реализации настоящей Стратегии предотвращаются за счет совершенствования безопасности функционирования информационных и телекоммуникационных систем критически важных объектов инфраструктуры и объектов повышенной опасности в Российской Федерации, повышения уровня защищенности корпоративных и индивидуальных информационных систем, создания единой системы информационно-телекоммуникационной поддержки нужд системы обеспечения национальной безопасности».

В сложившихся условиях вопросы обеспечения коллективной информационной безопасности в Российской Федерации приобретают особую актуальность, а их решение невозможно без грамотного научно-обоснованного подхода. Видится с одной стороны целесообразным теоретическое обоснование понятия национальной информационной безопасности Российской Федерации, и разработка Концепции национальной информационной безопасности Российской Федерации, сделав указанную концепцию составной частью Стратегии национальной безопасности Российской Федерации или выделив её в отдельный нормативно-правовой акт, а с другой стороны разработать эффективные организационно-правовые механизмы.