Е.А. Соловьева

Система информационного противоборства в сети Интернет: опыт современной России

Манипулятивные технологии Интернета как глобальной структуры и как явления в сфере политико-властных отношений, а также возможности и технологии их использования в процессе ведения сетевого информационного противоборства ярко высветили все правовые проблемы защиты интересов государства, общества, юридических и частных лиц РФ в сети Интернет, а также поставили задачу управляемости процессами использования государственных информационных Интернет-ресурсов в интересах укрепления технической и нормативно-правовой баз обеспечения информационной борьбы в сети Интернет как основы государственной системы сетевого информационного противоборства России.

Система органов государственной власти и управления Российской Федерации, будучи доминирующим фактором, регулирующим общественные отношения в информационно-психологической сфере, а, следовательно, и основой ведения информационного противоборства, является центральным звеном обеспечения информационно-психологической безопасности и основным инструментом отражения и пресечения любых посягательств политических акторов-оппонентов на суверенитет, целостность и гражданское единство российского общества, на его жизненно важные интересы и перспективы развития, на

психическое здоровье населения России.

В настоящее время виртуальное пространство в большинстве случаев повторяет реальную сферу политики, следствием чего является усиление конфронтации различных субъектов политики в борьбе за освоение новых ресурсов виртуального пространства. Данное обстоятельство обусловливает необходимость выработки на государственном уровне системных мер и механизмов противодействия негативному информационному влиянию в сети Интернет как основы обеспечения национально-государственной, общественной и личной безопасности, т.е. по сути позволяет говорить о формировании государственной системы информационного противоборства в виртуальном пространстве глобальной сети.

Исходя из понимания «системы» как совокупности, целого, составленного из частей, мы считаем, что каждая система должна включать в себя взаимодействующие части: подсистемы и элементы, где главное значение приобретают связи и отношения между частями данной системы.

В этой связи под российской государственной системой информационного противоборства в сети Интернет следует понимать централизованный, согласованный и целенаправленный комплекс мероприятий и механизмов органов государственной власти РФ, направленный на защиту государственных интересов и обеспечение личной, общественной и национальной безопасности России в сети Интернет.

Основу функционирования системы информационного противоборства России в сети Интернет составляют следующие компоненты (подсистемы и элементы), находящиеся в тесной взаимосвязи и взаимодействии друг с другом и обеспечивающие реализацию и правовое регулирование комплекса согласованных мероприятий информационного воздействия и противодействия:

1. институциональная база (органы государственной власти РФ и их структурные подразделения, ответственные за обеспечение безопасности в Интернете);
2. техническая база (механизмы реализации и контроля мероприятий информационного противоборства);
3. нормативно-правовая база (законодательные акты и инициативы в сфере управления сетью Интернет).

Институциональную базу системы ИП в сети Интернет России составляют структурные подразделения органов государственной власти РФ, отвечающие за обеспечение информационной безопасности России в сети Интернет, а также контроль и координацию СМИ. К ним относятся:

- в Совете Безопасности РФ: Управление информационной безопасности;

- в Правительстве: Министерство связи и массовых коммуникаций

РФ, в ведомстве которого, в частности, находится отраслевой Отдел по Интернету и новым СМИ; Федеральное агентство по печати и массовым коммуникациям, Роспечать, Росинформтехнологии, Россвязь, Россвязькомнадзор;

- в Федеральном Собрании: Комитет Государственной Думы по информационной политике, информационным технологиям и связи; Комиссия Совета Федерации по информационной политике;

- в Администрации Президента: Служба оперативной информации, Пресс-служба, Информационно-аналитический центр, Аналитический центр по социально-экономической политике.

Техническая база системы информационного противоборства (механизмы обеспечения ИП) включает в себя следующие основные компоненты:

1. Систему диагностики угроз и механизмов противодействия информационно-психологической агрессии на ранних стадиях информационного противоборства, а именно:

- комплекс первоочередных действий при начале информационной войны;

- инструменты отражения внезапного информационного нападения в Интернете («боевые» Интернет-блоги, построение «боевой» группировки).

2. Механизмы реализации комплекса ответных мер в условиях ожидаемых интернет-атак, а также систему быстрого реагирования на внезапно выявленные акции сетевой информационно-психологической агрессии. Сюда относятся

- основные приемы борьбы с информационными нападениями в Интернете,

- общие принципы работы с информацией;

- методы и принципы доведения до интернет-аудитории своей точки зрения (политическое манипулирование, семантические атаки);

- инструменты распространения негативной информации в Интернете (корпоративные и личные сайты, расположенные на платных и бесплатных хостингах, блоги, форумы, черные списки, сайты для размещения компромата, сайты-клоны и сайты-«подставы»).

3. Систему сил и средств планирования краткосрочных и затяжных информационных войн в глобальной сети. К данной группе механизмов относятся:

- использование традиционных оффлайновых инструментов и их адаптация к Интернету;

- стратегическое планирование комплекса мероприятий противодействия интернет-атакам;

- профилактические меры и подготовка к возможному нападению (обеспечение собственной анонимности в Интернете, законные способы маскировки IP);

- мониторинг изменений на сайтах-источниках и сайтах-агрессорах (RSS-агрегаторы, сторожевой робот WebSite-Watcher, программа Check@Get);

- методы конкурентной разведки в сети Интернет (изучение политического противника по «Архиву Интернет», визуальный поиск, использование сервиса Whols).

4. Государственная информационная политика по противодействию акциям (мероприятиям) информационно-психологической агрессии в сети Интернет.

Комплексное применение вышеперечисленных методов, приемов и политических технологий, подкрепленное скоординированной государственной информационной политикой, способствует организации эффективной борьбы с негативной информацией в сети Интернет.

Нормативно-правовая база обеспечения системы информационного противоборства России состоит из норм федерального законодательства, дающих юридическую квалификацию мероприятиям информационно-психологической агрессии в сети Интернет, относя их к категории противоправных действий, устанавливая степень их социальной опасности и определяя объем ответственности физических и юридических лиц за организацию, подготовку и пособничество в совершении этих деяний.

Сюда же относится и комплекс мероприятий, связанный с уточнением перечня и состава правонарушений, относящихся к организации или подготовке акций информационно-психологической агрессии в сети Интернет; разработкой механизмов проведения следствия и судебного разбирательства по фактам обнаружения противоправных действий в информационно-коммуникативном пространстве глобальной сети и порядком ликвидации последствий этих противоправных действий с учетом специфики уголовной, гражданской, административной ответственности и включением соответствующих правовых норм в уголовный, гражданский и административный кодексы Российской Федерации.

Помимо разработки внутренних правовых механизмов регулирования глобальной сети РФ участвует в разработке норм международного права, устанавливающих международную ответственность государств-агрессоров за совершение противоправных действий в сети Интернет.

Практика показывает, что причиной появления тех или иных законодательных инициатив в сфере интернет-регулирования в России нередко являлись прецедентные факты и события («Дело Поносова», «Дело Саввы Терентьева»), требующие от законодательных органов РФ

соответствующего правового реагирования и, таким образом, способствующие формированию и укреплению правовой базы системы информационного противоборства в сети Интернет.

В целом можно утверждать, что в настоящее время российская государственная система информационного противоборства в сети Интернет находится еще в стадии становления, о чем свидетельствует отсутствие комплексных правовых инициатив (Закон об Интернете, Концепция кибербезопасности и т.п.), исполнительных институтов, ответственных за обеспечение безопасности в сети Интернет (Центр информационного противоборства, система информационно-психологического обеспечения деятельности аппарата управления России), а также отдельных механизмов координации деятельности органов государственной власти и общества в сети Интернет (общественный Центр обработки данных об угрозах в Интернете или др.).

В силу всего вышесказанного можно сделать следующее заключение: в современных условиях существующая ныне система информационного противоборства РФ не в полной мере соответствует новым условиям общественного развития и, следовательно, не может в полной мере эффективно противодействовать угрозам виртуального пространства, используя прежние принципы управления.