КЛЮЧЕВЫЕ ЭЛЕМЕНТЫ РОССИЙСКОЙ СИСТЕМЫ ПРОТИВОДЕЙСТВИЯ ИНФОРМАЦИОННЫМ И КИБЕРАТАКАМ

Аннотация

В статье рассматривается история создания и развития национальной системы защиты от информационно-психологических операций в Российской Федерации как на государственном, так и на международном уровне. Автор приходит к выводу, что на сегодняшний день в РФ создана полноценная система защиты от проводимых иностранными государствами информационно-психологических операций, которая, однако, обладает рядом недостатков.

Ключевые слова: Россия, информационная война, ГПЭ, кибербезопасность, защита.

Автор

Курилкин Антон Владимирович

Корреспондент МИА «Россия сегодня», выпускник аспирантуры факультета государственного управления Московского государственного университета имени М.В. Ломоносова (Москва, Россия)

Определенной особенностью российского подхода к обеспечению информационной безопасности стал тот факт, что изначально Россия не стала создавать национальную систему защиты от информационного воздействия, а предложила принять определенные правила игры на международной арене в данной области — в 1998 г. в адрес Генерального секретаря ООН было направлено специальное Послание министра иностранных дел РФ И.С. Иванова по проблеме международной информационной безопасности [6].

В данном документе особый акцент был сделан на обеспечение международной информационной безопасности и предотвращение появления принципиально новой области конфронтации — информационного пространства. Российский МИД подчеркивал, что с учетом возрастающей информатизации общества возможно появление принципиально нового типа оружия — информационного, чье применение может оказаться сравнимым по последствиям с применением оружия массового поражения.

Последствием данной инициативы стало принятие Генеральной ассамблеей ООН резолюции A/RES/53/70 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Данная резолюция предлагала государствам — членам ООН обсудить вопросы информационной безопасности, предложить свои оценки проблемы и разработать международные принципы обеспечения информационной безопасности в мире. Свои предложения страны должны были передать Генеральному секретарю ООН для подготовки доклада.

10 августа 1999 г. был опубликован доклад Генерального секретаря ООН, который включил в себя оценки групп экспертов из Австралии, Беларуси, Брунея, Великобритании, Катара, Кубы, Омана, России, Саудовской Аравии и

США. Несмотря на то, что все вышеперечисленные страны признали наличие проблемы, группы экспертов сделали разные оценки военных, правовых и гуманитарных аспектов проблемы, в целом использовали при подготовке рекомендаций разные методики и, соответственно, предложили разные пути решения.

По итогам дальнейшей работы экспертных групп и с подачи России Генеральной Ассамблеей ООН был принята резолюция A/RES/55/28 и A/RES/56/19. В рамках этих документов был предложен ряд положений о продолжении дальнейшей экспертной работы и принято решение о создании специальной Группы правительственных экспертов (ГПЭ).

Основными задачами группы были определены: рассмотрение угроз в сфере информационной безопасности, исследование проблем укрепления безопасности глобальных информационных и телекоммуникационных систем, а также разработка возможных мер к их устранению.

Во время подготовки соответствующих предложений и в ходе первых заседаний ГПЭ активное противодействие предлагаемым мерам оказывали представители США. Как подчеркивает первый председатель ГПЭ, российский дипломат А.В. Крутских, объясняется это нежеланием Соединенных Штатов лишить себя свободы в применении информационно-коммуникационных технологий в военных целях и избежать разработки и принятия регламентирующего применения ИКТ международного законодательства [5].

С момента создания ГПЭ до публикации первого доклада прошло шесть лет — только в 2010 г. группа экспертов смогла предоставить первый документ по итогам работы. Следующая публикация доклада произошла в 2013 г.; третий доклад ГПЭ представлен в 2015 г.

В целом работа группы правительственных экспертов привела к достаточно значимым результатам — выработана (пусть и достаточно расплывчатая) нейтральная терминология, признан ряд проблем в области международной информационной безопасности, выработан ряд предложений по обмену информацией между странами по актуальному законодательству в области ИКТ, об инцидентах в области ИКТ, проработан механизм работы двусторонних, региональных и многосторонних площадок для обсуждения актуальных проблем ИКТ.

Однако, оценивая деятельность ИКТ, ряд экспертов [3], [8], [1] по данной проблематике подчеркивает, что деятельность ГПЭ, скорее, внесла большой вклад в продвижение проблематики ИКТ в контексте МИБ, а не в решение конкретных проблем.

Помимо деятельности в ООН по вопросам МИБ Российская Федерация активно налаживала сотрудничество по данной проблеме в двустороннем формате. В настоящее время в рамках региональных международных организаций (СНГ, ШОС, БРИКС и ОДКБ) подписан ряд договоров в области обеспечения МИБ. Аналогичные соглашения на двустороннем уровне заключены с Республикой Беларусь, Бразилией, Китаем, Кубой и Индией. Как отмечает ряд экспертов [11], формулировки в данных документах достаточно схожи, и в целом в их основу положены формулировки российского законодательства в данной сфере.

На примере работы ГПЭ и российских предложений можно выделить важную отличительную особенность российского подхода к проблеме обеспечения информационной и кибербезопасности — это упор на информационно-психологический аспект данной проблемы при использовании крайне обтекаемых и широких формулировок в аспекте проблем обеспечения безопасности инфраструктуры и, соответственно, действий в киберпространстве.

Определение информационной безопасности в национальном законодательстве

Под информационной безопасностью в России прежде всего понимается состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие РФ, оборона и безопасность государства [4].

Под информационной инфраструктурой прежде всего понимается совокупность объектов информатизации, информационных систем, сайтов в сети Интернет и сетей связи, расположенных на территории РФ, а также на территориях, находящихся под юрисдикцией РФ или используемых на основании международных договоров РФ [4].

Таким образом, можно сказать, что прежде всего в документах стратегического планирования (Доктрина информационной безопасности РФ, Концепции внешней политики РФ, Военная доктрина РФ, Основы государственной политики РФ в области международной информационной безопасности) понятие информационного пространства эквивалентно понятию киберпространства, использующегося в США, Китае и в ряде международных организаций.

Стоит отметить и тот факт, что изначально российский взгляд на проблему развивался на основе угроз информационно-психологического характера; значимое внимание проблемам киберпреступности, например, было уделено впервые в Концепции внешней политики РФ от 2013 г. При этом в документе по-прежнему остались неразделенными понятия киберугроз и информационных угроз социально-политической стабильности.

Попытка разделения подобных угроз была предпринята уже на международном уровне в соглашении между Правительством РФ и Правительством КНР о сотрудничестве в области обеспечения международной информационной безопасности от 30 апреля 2015 г. [9]. В тексте документа были выделены понятия объектов критической информационной инфраструктуры, компьютерной атаки, неправомерного использования информационных ресурсов и несанкционированного вмешательства в информационные ресурсы.

Такой подход отчасти объясняется пониманием разрушительности информационно-психологического воздействия на примере опыта цветных революций на постсоветском пространстве, опыта «пятидневной войны» и «арабской весны», однако стоит отметить, что российским взглядам присущ определенный консерватизм в видении внешнеполитической реальности и чрезмерное внимание к роли государства в данной проблеме.

В 2012 г. в России был принят федеральный закон № 139-ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации по вопросу ограничения доступа к противоправной информации в сети Интернет» [10]. После принятия этого закона был создан «Единый реестр доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено» — автоматизированная система для блокировок сайтов с запрещенной для распространения на территории России информацией.

Стоит отметить и тот факт, что в 2014 г. были приняты поправки в закон о СМИ, согласно которому было ограничено участие иностранных граждан

и государств во владении средствами массовой информации, вещающими в России [7].

О понимании необходимости защиты собственных информационных систем российским руководством свидетельствует и создание нового вида войск в структуре Вооруженных сил РФ — войск информационных операций [2]. Однако, как подчеркнул министр обороны России С. Шойгу, главной задачей данных войск станет прежде всего контрпропаганда.

Определенной вехой в создании системы информационной и кибербезопасности стало принятие двух достаточно резонансных законопроектов — о «суверенном Рунете» (который предполагает создание национальной резервной инфраструктуры для работы Интернета и различных телекоммуникационных сетей в случае ограничения доступа России к соответствующей зарубежной инфраструктуре) и «закона о фейках», который устанавливает ответственность за распространение недостоверной общественно значимой информации.

Кроме работы с «внутренней аудиторией» российскими властями широко используются и возможности Интернета для вещания на зарубежную аудиторию с целью информирования о происходящих в стране событиях и донесения точки зрения РФ на происходящие события в мире. Первым подобным СМИ стал созданный 10 декабря 2005 г. телеканал «Russia Today». С момента создания телеканал неоднократно критиковался западными политиками в связи с якобы необъективной подачей информации и предвзятости в освещении событий, однако данные обвинения не подтверждались конкретными доказательствами. На сегодняшний день телеканал вещает более чем в 100 странах мира на пяти языках: английском, арабском, испанском, русском и французском. Все трансляции ведутся, в том числе, и в Интернете.

В 2013 г., указом президента России В. Путина [12] в целях повышения эффективности деятельности государственных средств массовой информации были реорганизованы и объединены в информационное агентство «РИА Новости» и государственная радиовещательная компания «Голос России» (вещавшая в первую очередь на зарубежную аудиторию). В созданном на основе объединенных СМИ холдинге МИА «Россия сегодня» было, в свою очередь, в 2014 г. создано новое подразделение, отвечающее за вещание на зарубежные аудитории информационное агентство и радио Sputnik. В настоящий момент ИА Sputnik вещает более чем в 30 странах мира на 31 языке.

В докладе американских спецслужб [13] работа Russia Today и Sputnik неоднократно критиковалась за пропаганду и вмешательство в электоральные процессы в США и ряде стран ЕС. Кроме того, в ряде американских и европейских СМИ неоднократно утверждалось, что «Кремлю удалось создать самую мощную пропагандистскую машину XXI века».

Таким образом, на анализе предложенных РФ на международном уровне соглашений, договоров и конвенций можно сказать, что руководством РФ не рассматриваются в отдельности проблемы обеспечения кибербезопасности — речь идет прежде всего о комплексной информационной безопасности, которая включает в себя как угрозы для нормального функционирования информационно-коммуникационной среды, так и угрозы информационно-психологического плана.

При этом гораздо большее внимание уделяется вопросам защиты от информационного влияния, нежели чем защиты собственной интернет-инфраструктуры и ключевых элементов информационной инфраструктуры, что создает уязвимости в национальной системе киберзащиты. Более того, в условиях ухудшившейся социально-экономической ситуации на первое место выходит не столько вопрос противостояния зарубежным инфор-

мационным атакам, сколько создания и продвижения альтернативного контента и «борьбы за умы» внутри страны.

Кроме того, Россия уделяет значительное внимание и проблемам донесения до зарубежной аудитории и собственных взглядов, и позиций на происходящие в мире события, свидетельством чего является создание государственных СМИ, вещающих на зарубежные аудитории, и борьба со СМИ, вещающими на территории России и получающими средства от других государств. Тем не менее в условиях серьезного противостояния со стороны онлайн-платформ на западе инструменты продвижения российской повестки дня теряют возможности влияния, что создает необходимость корректировки модели вещания и продвижения.

Литература

1. *Бойко С.* Формирование системы международной информационной безопасности: российский подход и инициативы // Международная жизнь. — 2018. — № 5. — С. 100–110.
2. В России созданы войска информационных операций [Электронный источник] // Информационное агентство РИА Новости [Официальный сайт]. — URL: https://ria.ru/defense_safety/20170222/1488596879.html (дата обращения: 25.04.2018).
3. *Демидов О.* Обеспечение международной информационной безопасности и российские национальные интересы // Индекс Безопасности. — 2013. —№ 1 (104). — С. 129–168.
4. Доктрина информационной безопасности Российской Федерации (Утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895) [Электронный ресурс] / Информационно-правовой портал «ГАРАНТ» [Офиц. сайт]. — URL: http://base.garant.ru/182535/ (дата обращения: 25.04.2018).
5. *Крутских А.* Кто владеет Интернетом, тот владеет миром // Международная жизнь. — 2016. — № 11. — С. 18–27.
6. Международное сотрудничество в области информационной безопасности [Электронный ресурс] / Министерство иностранных дел Российской Федерации [Офиц. сайт]. — URL: http://www.mid.ru/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/486848/ (дата обращения: 25.04.2018).
7. Поправки вносятся в статью 6 Закона «О средствах массовой информации» [Электронный источник] // Российская газета [Официальный сайт]. — URL: https://rg.ru/2014/10/17/ino-smi-dok.html (дата обращения: 25.04.2018).
8. Проблемы информационной безопасности в международных военно-политических отношениях / Под ред. А.В. Загорского, Н.П. Ромашкиной. — М.: ИМЭМО РАН, 2016. — 183 с.
9. Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности [Электронный ресурс] / Правительство Российской Федерации [Офиц. сайт]. — URL: http://static.government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf (дата обращения: 25.04.2018).
10. Федеральный закон от 28 июля 2012 г. № 139-ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации» [Электронный ресурс] / Российская газета [Офиц. сайт]. — URL: https://rg.ru/2012/07/30/zakon-dok.html (дата обращения: 25.04.2018).
11. Угрозы информационной безопасности в кризисах и конфликтах XXI века / Под ред. А.В. Загорского, Н.П. Ромашкиной. — М.: ИМЭМО РАН, 2015. — 151 с.
12. Указ о мерах по повышению эффективности деятельности государственных СМИ [Электронный источник]// Официальный сайт Президента России [Официальный сайт]. — URL: http://kremlin.ru/events/president/news/19805 (дата обращения: 25.04.2018).
13. Worldwide threat assessment of the US Intelligence Community [Электронный ресурс] / Office of the Director of National Intelligence [Офиц. сайт]. — URL: https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf (дата обращения: 25.04.2018).