УДК 343.92

ПРОФИЛАКТИКА И БОРЬБА С КИБЕРТЕРРОРИЗМОМ В КИТАЕ. КИТАЙСКИЙ ОПЫТ В РОССИИ

PREVENTION AND COMBATING CYBERTERRORISM IN CHINA. THE CHINESE EXPERIENCE IN RUSSIA

Е.Ю. Макарова, А.А. Василенко
E. Y. Makarov, A. A. Vasilenko

Белгородский государственный национальный исследовательский университет, Россия, 308015, г. Белгород, ул. Победы, 85
Belgorod State National Research University, 85 Pobeda St., Belgorod, 308015, Russia

E-mail: makarova9liza@yandex.ru;

Ключевые слова: кибертерроризм, терроризм, Китай, Россия, ООН, резолюции ООН, Золотой щит, информация, интернет, кибербезопасность.
Key words: cyberterrorism, terrorism, China, Russia, UN, UN resolution, The Golden Shield Project, information, internet, cybersecurity.

Аннотация. В статье рассматривается феномен интернет-преступности, киберпреступности с позиции надгосударственного явления; виды профилактики кибертерроризма.
Abstract. The article discusses the phenomenon of Internet crime, cybercrime from the position of a supranational phenomenon; prevention of cyberterrorism.

Интернет является важным инструментом не только для объединения разных мировых культур, но и для обмена между ними различного рода информацией: экономической, политической, торговой и так далее. Совершенствование информационных технологий дает толчки для развития любого государства, а пользователи всемирной сети Интернет приобрели новые возможности массового распространения идей и обмена информацией. За последнее время количество людей пользующихся интернетом выросло и продолжает расти. Вместе с активными пользователями сети множатся и преступные элементы, а так же различные запрещенные террористические организации. Они используют это пространство для увеличения своего влияния, распространения различной информации насильственного характера, различных заявлений и прочих неправомерных действий. Преступники постоянно используют интернет для влияния на общественное сознание [1].

Международное сообщество отреагировало на кибертерроризм следующими мерами. ООН (Генеральная Ассамблея, Совет Безопасности) приняли ряд резолюций, которые призывают все мировое сообщество к сотрудничеству в борьбе с терроризмом. Так в июне 2014 года была рассмотрена и принята на 68 сессии ООН «Глобальная контртеррористическая стратегия». В ней по инициативе Китая были внесены и включены поправки о киберрпреступности [2].

Для начала, международное сообщество не пришло к консенсусу в определении понятия «кибертерроризм» и именно это замедляет разработку системы борьбы с данным явлением. Впервые понятие кибертерроризма вводится научным сотрудником Калифорнийского института безопасности и разведки в 1996 году. С этого времени началось активного изучение данного феномена и большая часть научного сообщества обозначает его как надгосударственное явление, целями и результатами которого является реализация и организация насильственных действий.

Так как киберпреступность является международным явлением, необходимо принять меры для обозначения четких регламентированных стандартов в определении понятия кибертерроризм. Если укреплять международное сотрудничество в борьбе против кибертеррористических актов в рамках конвенций ООН, то появляется необходимость в новых условиях развития международных отношений и установления согласия между всеми странами участниками.

Правительство Китая в борьбе с киберпреступностью использует несколько мер и средств. Так в 1 июля 2015 года был принят «Закон о национальной безопасности КНР», 6 июля 2015 стартовал проект закона «О безопасности в Интернете», в декабре того же года был принят «Закон о борьбе с терроризмом». Эти законопроекты несут в себе правовую почву в борьбе с данным видом преступности. Китаем были проведены исследования западных коллег, в частности США, Евросоюза, Германии, Великобритании и других [3]. В 2016 году «Закон о борьбе с терроризмом»

был реализован и введен в действие. Согласно этому закону правительство обеспечивает гарантии по выявлению различных видов террористической информации на просторах Сети.

Интернет-операторы Китая, которые являются поставщиками услуг под руководством правительства обязуются подвергать очистке информацию в интернете. Существуют ряд интернет-предприятий, которые специализируются на исследованиях информации в потенциально-опасных зонах.

Граждане и общественные организации так же вовлечены в борьбу с неправомерными действиями террористов. Так, например, во время олимпиады в Пекине 2008 года была запущена система поощрений граждан за предоставления какой-либо информации о возможных терактах. Некоторые сайты содержат в себе платформы для размещения людьми или же общественными организациями сообщений о незаконной информации. Для реализации борьбы со стороны населения необходима гласность и образование граждан. Помимо Департамента по борьбе с терроризмом, каждый человек может быть полезным в борьбе и оказать помощь и содействие. Так же необходимы специальные технологии, которые помогут фиксировать и вычислять потенциальные угрозы. Увеличение числа камер видеонаблюдения, тщательная оборона специальный предприятий (производство нефтепродуктов, опасных веществ и прочие) входят в комплекс мер по предотвращению терактов.

Существует национальный центр информации о борьбе с терроризмом, в котором происходит сборка информации, координация, исследования. Все остальные отделы собирают и направляют информацию центру по борьбе с терроризмом. Самым важным моментом «Закона по борьбе с терроризмом» является активный сбор и использование информации. Таким образом, террористическая деятельность может быт подавлена в зачаточной стадии. Ведь именно своевременное выявление и непосредственное оперативное вмешательство гарантирует благоприятный исход дела.

Китай планирует наладить сотрудничество с правоохранительными службами других стран для активной борьбы с интернет-преступностью и киберртерроризмом в целом. В опубликованной «Международной стратегии по сотрудничеству в киберпространстве» указывается следующее: "Китай усилит политический обмен и сотрудничество с правоохранительными органами других стран по киберпреступности и кибертерроризму" [4]. Так же в данном документе отмечается, что КНР планирует реализовывать двухстороннее сотрудничество с полицией других государств, содействовать обмену опытом по борьбе с киберпреступностью и развивать технологии. Согласно этому документу, Китай собирается совместными усилиями с другими государствами производить изучение мер по борьбе с киберпреступностью, а так же вести активное обсуждение конвенций для прихода к согласию в данной сфере. Для этих целей Китай планирует усиление сотрудничества со странами-участниками БРИКС, ШОС и АСЕАН [5].

Вслед за китайскими коллегами в России в последнее время постоянно нарастают попытки взять под контроль регулирующих органов российский сегмент интернета. Более того, иногда желания регулирующих органов не всегда распространяются на русские ресурсы, но и иногда на иностранные ресурсы и компании. Подобная тенденция уже почти ни у кого не оставляет сомнений, что правительство и специальные подразделения взяли курс на построение аналога «Великого Китайского Фаервола», который на сегодняшний момент считается самым совершенным механизмом государственного контроля Интернета. Его разработка началась еще в 1998 году, начал работу в 2003, однако был полностью институализирован только в 2006-м. Российский аналог – реестр Роскомнадзора – начал работу по блокировке в 2012 и в этом году отчитался о 275 тысячах заблокированных ресурсов [6].

«Золотой щит» осуществляет мониторинг как внешних, так и внутренних сайтов. Он же осуществляет блокировку доступа несколькими методами, которую хоть и возможно обойти, но это довольно сложная задача.

Согласно описанным выше китайским законам, китайские ресурсы несут ответственность за легитимность информации и, более того, все новости они должны цитировать только со специальных медиа-ресурсов, включенных в своеобразный «белый список».

Китайский фаервол пока опережает российский блокировщик и с точки зрения технического исполнения, и с юридической точки зрения тоже, однако российские законотворцы делают все, чтобы его улучшить. Так, например, в июле 2016 года был принят «закон Яровой-Озерова» [7], призванный решить сразу несколько задач в борьбе с терроризмом, экстремизмом, кибертерроризмом и распространением не законной информации. Несмотря на сильнейшую критику экспертами и населением, на возможные серьезные негативные последствия принятых мер и на предстоящие колоссальные финансовые затраты для технической реализации, оцениваемые вплоть до 33 млрд. дол. США, его реализация уже началась, поскольку безопасность интернета декларируется сегодня как один из приоритетов внутренней политики России.

По словам члена Совета Федерации Федерального Собрания Российской Федерации Ф. Клинцевича, масштабы сегодняшних хакерских атак впечатляют и неизвестно, что будет

происходить дальше, какие требования могут выдвинуть террористы. Мы уже были свидетелями ударов по компьютерам больниц, железнодорожного транспорта, МВД, добавил сенатор. "Надеюсь, что уже не надо никого убеждать. Если мы – человечество – не осознаем эту угрозу и не объединим усилия по ее пресечению, то нас ждут очень большие неприятности. Этот вид терроризма вообще не имеет границ и не знает никаких, кроме технических, преград. В эти дни мир получил серьезнейшее предупреждение", — заключил Клинцевич [8]. Россия – не единственное государство, движущееся к регулированию своего сегмента сети и его обособлению. Подобные меры считаются большинством стран необходимыми в связи с все более нарастающей угрозой кибертерроризма.

На данный момент существует необходимость выявить на теоретическом и прикладном уровнях проблем, связанных с информатизацией. Э. Тоффлер, Д. Белл, Ф. Фукуяма, Й. Масуда говорили в своих работах о наступлении нового витка развития цивилизации, которая неразрывно связана с информатизацией и глобализацией.

Э. Тоффлер указывал, что информация станет источником власти в политике новой цивилизации. Так как политика является своеобразной битвой за власть, ее сохранение и укоренение, то информация будет являться главным оружием в этой борьбе. «Мы живем в момент, когда вся структура власти, скреплявшая мир, дезинтегрируется. Совершенно новая структура обретает форму. И это происходит на всех уровнях человеческого общества. Это крушение старого стиля управления ускоряется также в деловой и повседневной жизни, когда дезинтегрируются глобальные структуры власти» [9]. Что мы можем видеть на сегодняшний день, информация является источником и ресурсом власти. Информация управляет жизнедеятельностью государств всего мирового сообщества, а информационные технологии применяются в разных сферах и для решения разных задач, в особенности связанных с безопасностью (национальной, экономической, военной и прочее). Противоборство в информационной сфере становится сферой противоборства даже между государствами [10]. Совсем не удивительно, что этим же могут воспользоваться и преступные организации.

На данном этапе требуется провести полный анализ современной информационной и политической ситуации в мире и в частности в России, прогнозировать изменения в этих сферах. Так же необходимо досконально изучить влияние информационных средств, технологий на политическую и международную коммуникацию, каким образом происходит влияние на эти сферы, найти пути решения проблем. Для реализации активной борьбы и профилактики терроризма существует необходимость поиска и представление Россией стратегий мировому сообществу, и реализовывать ее совместно с другими государствами.

Список литературы
References

1. Как современный терроризм использует Интернет: специальный доклад № 116 // Вейманн Г. Владивостокский центр исследования организованной преступности. 2004.
2. Глобальная контртеррористическая стратегия Организации Объединенных Наций: резолюция Генеральной Ассамблеи ООН от 08.09.2006. URL: http://docs.cntd.ru/ document/902114207
3. Контртерроризм в Китае необходим. URL: http://www.Legaldaily.Com. /cn/commentary/ content/2015-12/29/content_6423984.node=33188.Htm?Node=33188
4. Обзор к уголовного законодательства о борьбе с терроризмом и «Закона о борьбе с терроризмом» Китая» / Евразийский Научный Журнал, №5, 2016 (май). Цзан Цземэй
5. Китай усилит сотрудничество с другими странами в борьбе с кибертерроризмом. URL: https://ria.ru/world/20170302/1489084186.html
6. Роскомнадзор за пять лет заблокировал около 275 тыс. ресурсов с запрещенной информацией URL: http://tass.ru/politika/4445476
7. Федеральный закон от 06.07.2016 г. № 374-ФЗ URL: http://kremlin.ru/acts/bank/41108
8. Клинцевич назвал массовые хакерские атаки кибертерроризмом. URL: https://ria.ru/society/20170513/1494239750.html
9. Тоффлер Э. Метаморфозы власти / Пер. с англ. М.: АСТ, 2001. 334 с. С. 23
10. Кибербезопасность как основной фактор национальной и международной безопасности 21 века (часть 1) / Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Вопросы кибербезопасности, 2013.