Изображение России в западной прессе в связи с киберконфликтами последнего десятилетия

Исследование Powerscourt, London
специально для НП «РАЭК»

Москва, май 2010

Вступление

Это исследование было выполнено исследовательской компанией Powerscourt (Великобритания, Лондон) по заказу Российской ассоциации электронных коммуникаций (РАЭК). Цель исследования — проанализировать изображение российской ИТ- и интернет-индустрии в контексте киберконфликтов в ведущих западных изданиях за последнее десятилетие — в период с начала 2000 года до конца марта 2010 года. Исследование охватывает новостные и аналитические материалы на тему киберпреступности, кибербезопасности, хакинга, спама и распространения вредоносных программ, имеющие отношение к России. Хотя со временем менялось количество, частота и содержание публикаций, можно заключить, что западная пресса, а значит, и весь западный мир до сих пор воспринимают Россию, как страну дикой киберпреступности, и со временем это убеждение только крепнет. Результатом такого восприятия в долгосрочной перспективе может быть заметное снижение инвестиционной привлекательности российской ИТ-отрасли, что может быть особенно болезненным в условиях, когда государство ориентируется на развитие и поддержку инновационной экономики.

Краткий обзор

В этом исследовании выявлены два основных тематических направления для публикаций на тему киберконфликтов, связанных с Россией.

Первое — геополитическое. Публикации на тему киберпреступности в западной прессе были более заметными и объемными в том случае, если их можно было связать с более значимыми темами для зарубежных отделов ведущих газет. В связи с этим первая волна интереса к российской киберпреступности была отмечена исследователями в середине 2000 годов, когда большую роль в российской политике начали играть олигархи, и западная пресса все больше сообщала об организованной преступности в России. Еще более заметная волна публикаций была зарегистрирована в последние годы в связи с ростом противостояния между Россией и Западом в связи с активными действиями США на территории бывшего СССР — в Грузии и на Украине. Тогда западная пресса высказывала предположения, что российское ИТ-сообщество — это русская армия хакеров, которая воюет за свою страну на виртуальных просторах интернета. Речь, в частности, идет об DDoS-атаках, которые сделали недоступными множество грузинских сайтов.

Второе направление состоит из публикаций, сообщающих об отдельных проявлениях «хакеров с дикого Востока», которые отличаются искусностью и особым коварством, и грозят посеять хаос в информационном обществе запада. Ранние примеры таких случаев — это известное дело Василия Горшкова (2000 год) и глобальная эпидемия вируса MyDoom (2004 год), в создании которого западные СМИ подозревают неизвестных российских программистов.

Сейчас интернет в западной прессе изображается, как поле битвы между ведущими странами мира, и это означает, что в ближайшем будущем российским интернет-компаниям будет очень трудно изменить представление, которое благодаря медиа сложилось о них на Западе. Это значит, что для всей российской интернет- и ИТ-отрасли в западном медийном пространстве формируется образ нецивилизованного и нерегулируемого пространства, которое грозит кибератаками всему миру.

Методология исследования

В основе данной работы лежит контент-анализ всех крупнейших газет и журналов США — The Wall Street Journal, New York Times, Washington Post, USA Today, Time, Newsweek, The Economist Fortune, Business Week, а также ведущих городских газет всех крупнейших американских мегаполисов. По аналогии с этим принципом отбора в рамках исследования также были проанализированы все крупнейшие газеты Великобритании, Германии, Франции, Италии и Испании. В исследование также попали публикации ведущих англоязычных печатных изданий следующих стран: Канада, Ирландия, Австралия, Новой Зеландия, Южная Африка, Сингапур, Гонконг и Объединенные Арабские Эмираты.

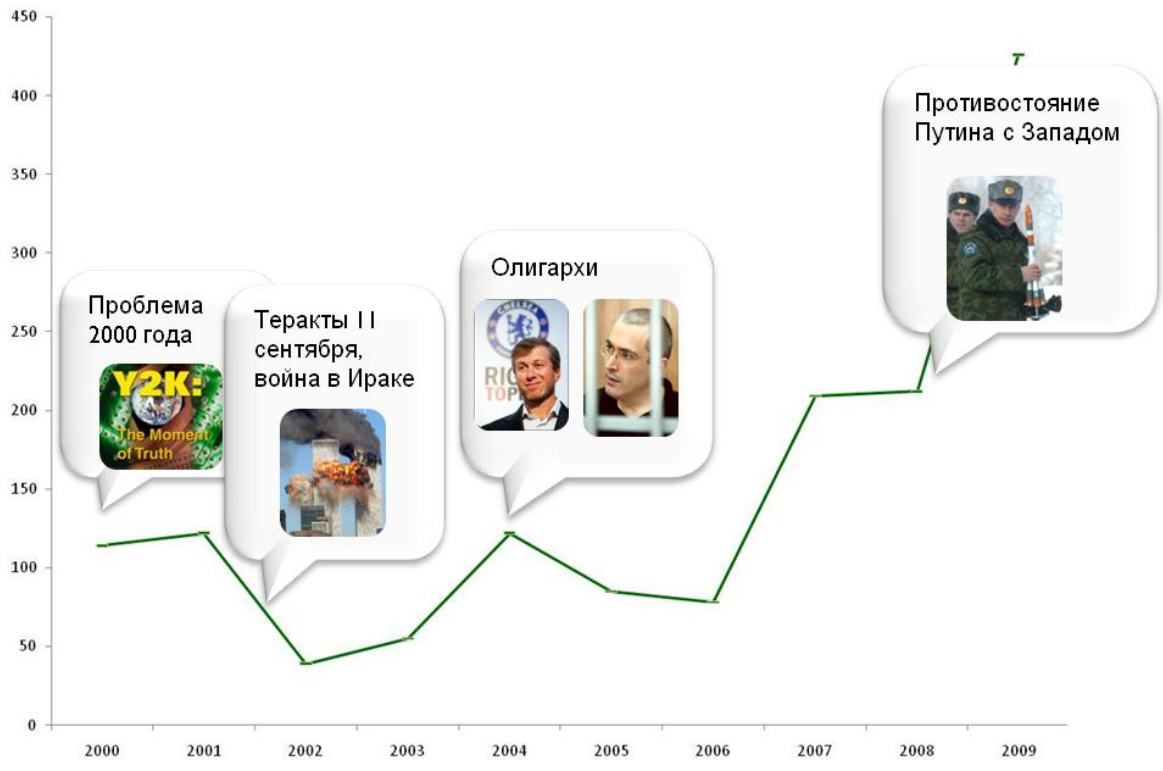
Поиск публикаций производился по ключевым словам: «киберпреступность», «кибербезопасность», «кибервойна», «хакинг», «фишинг» (выманивание паролей и персональных данных), «ботнет» (управляемая сеть, состоящая из зараженных компьютеров), «вредоносное программное обеспечение», «клик-фрод» (мошенничество, вынуждающее пользователя совершать клики на рекламные объявления). Если значительная часть текста была посвящена России, то он относился к категории публикаций, посвященных российской киберпреступности. Все прочие тексты вошли в категорию «публикаций на тему киберпреступности в целом».

Тематические направления публикаций: геополитический тренд

Число публикаций на тему киберпреступности, кибербезопасности и спама, связанных с Россией, за последнее десятилетие неравномерно, но стабильно росло. Заметный рост интереса западной прессы к данной тематике начался в 2006 году, и с тех пор число публикаций на тему российской киберпреступности постоянно увеличивалось. За весь период наблюдений количество публикаций, где упоминаются киберконфликты с участием России, выросло почти в 4 раза — со 114 в 2000 году до 426 в 2009 году. Можно предположить, что в этом году показатель 2009 года будет превзойден, так как лишь за первый квартал 2010 года западные СМИ выпустили 128 публикаций на тему российской киберпреступности. Как будет видно из исследования, со временем менялись характер и содержание данных публикаций. За счет чего сейчас в западном мире проблема российской киберпреступности выглядит значительно серьезнее, чем это было 10 лет назад. Причем консенсус западных СМИ состоит в том, что Россия является угрозой для цивилизованного мира в сфере высокотехнологичной деятельности и, прежде всего, интернета.

Публикации в СМИ: ориентир на модные темы

График №1: количество публикаций на тему киберконфликтов с участием России



Из графика №1 видно, что уровень интереса западной прессы к теме киберпреступности и кибербезопасности за весь период исследования находился в прямой зависимости от наиболее актуальных глобальных тем, которые интересовали СМИ на протяжении последней декады. В начале десятилетия все человечество было обеспокоено так называемой «Проблемой 2000 года». Поэтому совершенно неудивительно, что в СМИ появилось большое число статей, связанных с возможными сбоями в компьютерных системах. Публикации о хакерах и спаммерах в контексте общего возросшего к компьютерам интереса были весьма распространены.

Со временем стало ясно, что проблема 2000 года сильно преувеличена, и интерес к ней и к теме киберпреступности в целом стал снижаться. После чего ряд громких международных событий — террористические атаки на США 9 сентября 2001 года и последующее вторжение США в Афганистан и Ирак — вытеснили тему информационных технологий с первых полос западных газет.

Впрочем, уже к середине 2003 года наметился очередной подъем интереса к теме российской киберпреступности. На этот раз в связи с заметным ростом влияния на международной сцене российских олигархов — Михаила Ходорковского, Романа Абрамовича и других персонажей с интересным и ярким прошлым. В связи с этим в западной прессе стало появляться все больше материалов на тему организованной преступности из России, что и подстегнуло спрос на публикации, связанные с хакингом и рассылкой спама российскими киберпреступниками.

В то же время настоящий рост числа публикаций на тему киберпреступности и кибербезопасности произошел в 2006 году, когда у путинской России стало появляться все больше политических разногласий с западом по наиболее болезненным темам — поставкам газа в Европу, расширения НАТО на восток, усиления влияния США в Грузии и на Украине. На фоне этой политической борьбы западные издания охотно публиковали истории, где именно российское правительство обвинялось в кибератаках и кибершпионаже. Большинство этих публикаций носили безусловно пропагандистский характер, однако это не учитывалось в статистике и построении рейтинга, так как аудитория западной прессы лишена возможности альтернативного взгляда на происходящие события.

2000-2010: от киберпреступления к кибервойне

График №2: содержательные изменения в публикациях западной прессы о России

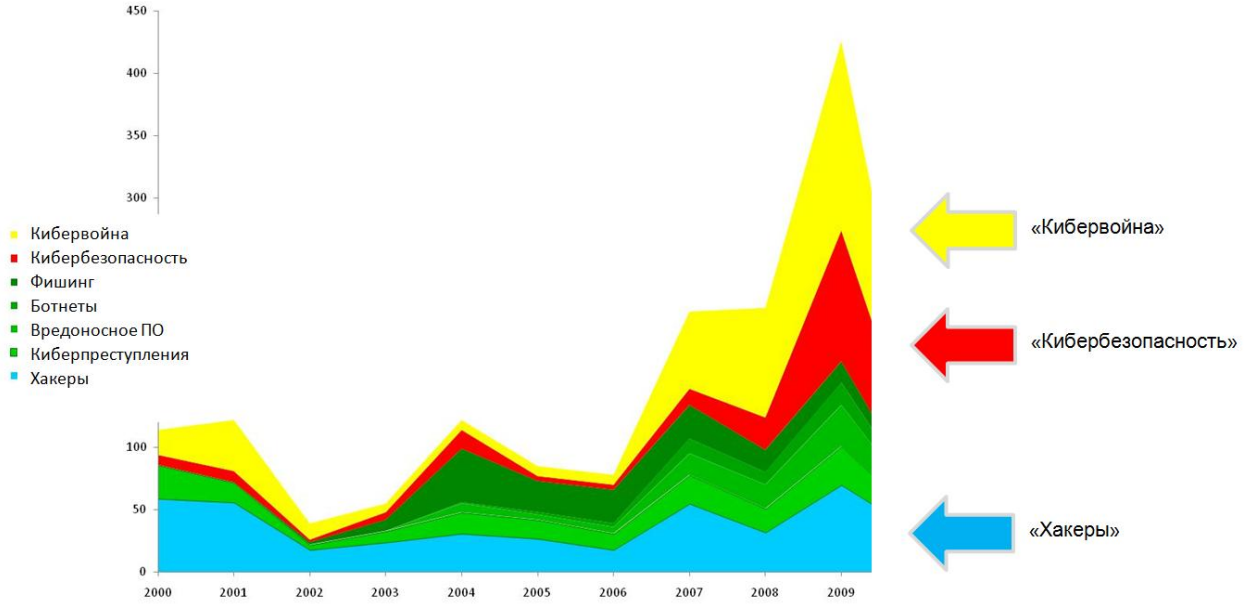


График №2 и Таблица №1 ниже показывают изменения в характере и содержании публикаций по теме российской киберпреступности. Из представленных на графике и в таблице данных видно, что в начале десятилетия большинство публикаций на обозначенную тему было связано с деятельностью частных лиц — независимых хакеров и небольших мошеннических групп, действовавших в своих интересах. С течением времени образ российского киберпреступника изменился, и акцент в освещении этой темы переместился в направлении геополитики. Ближе к концу первого десятилетия 2000-х годов образ киберпреступления трансформировался, превратившись из частной деятельности в государственную политику. В глазах западной прессы вопросы кибербезопасности и киберугроз отныне являются вопросами прежде всего политическими, а не просто криминальными.

Таблица №1: категории публикаций на тему киберконфликтов, тематическое распределение

Годы	Хакеры	Кибер-преступления	Вредоносное ПО	Ботнеты	Фишинг	Кибер-безопасность	Кибер-война	*Всего*
2000	59	27	0	0	0	8	20	***114***
2001	56	16	0	0	0	9	41	***122***
2002	18	4	0	0	2	2	13	***39***
2003	24	9	0	0	9	6	7	***55***
2004	31	17	7	1	43	15	8	***122***
2005	27	15	4	2	25	4	8	***85***
2006	18	13	5	3	27	4	8	***78***
2007	55	23	17	12	27	13	62	***209***
2008	32	19	19	10	18	26	88	***212***
2009	70	31	33	18	17	105	152	***426***
2010, 1Q	32	13	10	5	5	29	34	***128***

Россия как источник киберугроз

Рост использования интернета и компьютеров по всему миру изменил отношение общества к ИТ-тематике. За последнее десятилетие публикации на тему кибербезопасности и киберпреступности постоянно набирали популярность вне зависимости от того, имели они отношение к России или нет. Однако Россия, изображаемая обычно, как гнездо мировой киберпреступности, все больше появлялась в повестке дня мировых СМИ. График №3 (зеленая линия) демонстрирует общее количество публикаций на тему киберпреступности и число публикаций на данную тему, связанных с Россией (синяя линяя). На графике можно отметить любопытный момент: количество публикаций, связанных с Россией незначительно снизилось за последние десять лет на 5%, однако доля статей, посвященных России достаточно стабильна и до сих пор каждая седьмая публикация на тему киберпреступности посвящена нашей стране.

График №3: сравнение общего числа публикаций на тему киберконфликтов и публикаций, связанных с Россией

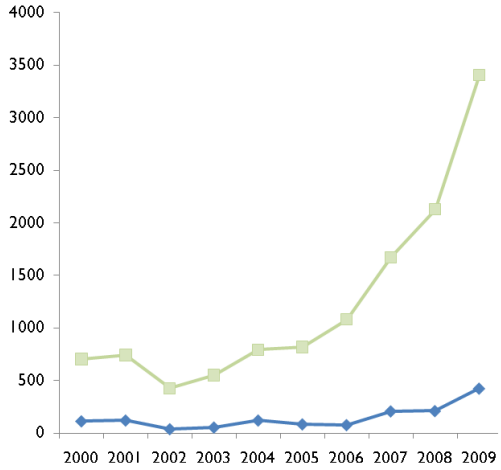
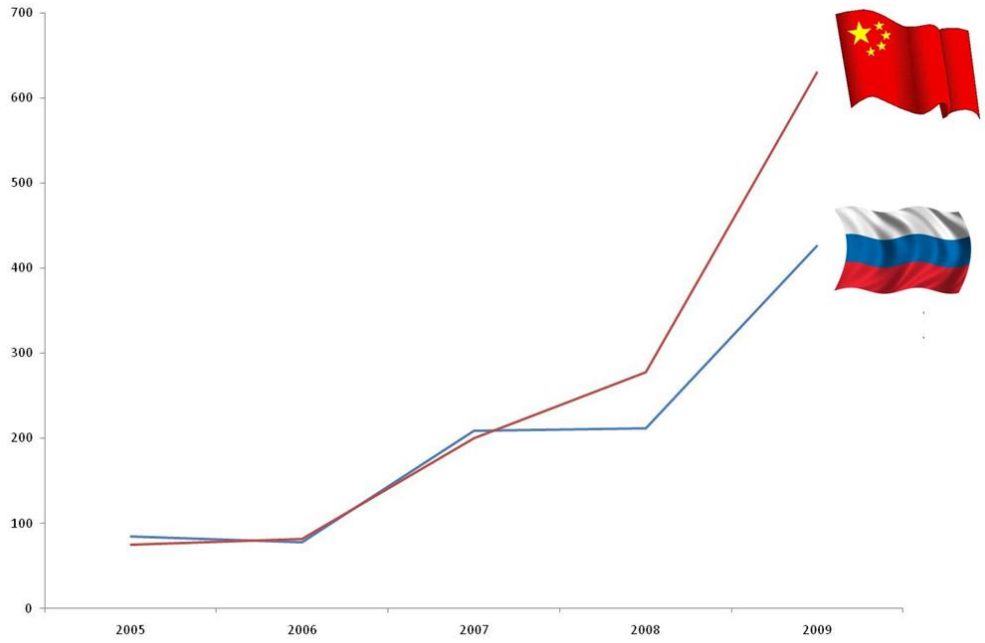


Таблица №2: соотношение общего числа публикаций на тему киберпреступности с публикациями о России

Годы	Публикации, связанные с Россией	Общее число публикаций	*Публикации о России от общего числа*
2000	114	590	***19%***
2001	122	622	***20%***
2002	39	387	***10%***
2003	55	496	***11%***
2004	122	671	***18%***
2005	85	735	***12%***
2006	78	1004	***8%***
2007	209	1463	***14%***
2008	212	1917	***11%***
2009	426	2982	***14%***

В последние годы, тем не менее, число публикаций о российской киберпреступности, росло в абсолютном отношении. Это связано с формированием мнения в западных СМИ о том, что кибервойна — это один из возможных способов международной конкуренции. В этом контексте Россия — давний противник Запада во всех прочих направлениях— неизбежно становится врагом и в киберпространстве. Особенно во время, когда отношения Путина и Медведева с Европой и США охладели. Впрочем, по той же самой причине на роль первого и главного соперника запада в кибервойне выходит Китай, который постепенно вытесняет Россию из публикаций на тему киберпреступности и становится еще большей страшилкой для западного общества. Это хорошо видно из графика №4: примерно три года назад Китай по числу публикаций на тему киберпреступности обогнал Россию и к текущему моменту только увеличил отрыв по данному показателю.

<u>График №4: Китай начал выходить на роль главного кибервраг Запада в 2007 году</u>



Главные события десятилетия

В исследовании уже отмечалось, как геополитические события или события большой мировой значимости — как, например, рост организованной преступности в России или обеспокоенность Пентагона кибервойной — способствовали созданию неблагоприятного имиджа России на международной арене. За последнее десятилетие произошло также несколько менее значимых событий, которые, тем не менее, нанесли серьезный ущерб репутации нашей страны и сформировали образ страны дикой киберпреступности. Герои новостей сгенерировали информационные пики. Разберем каждый из них отдельно.

2000: Мошенники и авантюристы

В самом начале десятилетия крупные порталы eBay и Yahoo сильно пострадали от сильнейших кибератак. Пресса связала это с действиями «неизвестных хакеров из России». Цены на акции обеих компаний после инцидента заметно снизились, а сам случай спровоцировал большое количество публикаций в январе-феврале 2000 года.

Шесть месяцев спустя интерес западной прессы к российским информационным специалистам вновь возрос. Это было связано с широкой общественной кампанией «Свободу Дмитрию», которая была запущена в поддержку программиста компании «Элкомсофт» Дмитрия Склярова в связи с его арестом в США. Склярова арестовали на выставке в Лас-Вегасе по обвинению компании Adobe за взлом защиты файлов популярного формата PDF. Кампания оказалась успешной, и обвинения со Склярова были сняты, однако в западном обществе закрепилась идея о том, что российское ИТ-сообщество является высокообразованным, но анархичным и неуправляемым. Кроме того, оно может представлять реальную угрозу для западной экономики.

Этот образ был закреплен позднее — осенью 2000 года, когда ФБР поймало российских хакеров Василия Горшкова и Алексея Иванова. Хакеры производили взлом сетей западных компаний, а потом представлялись специалистами по безопасности, способными устранить уязвимости. Несогласных шантажировали. По оценкам ФБР, заработки хакеров составили около 25 миллионов долларов.

2004: многомиллионные убытки

Если в 2000 году деятельность киберпреступников в описании западной прессы выглядела как разрозненная и хаотичная, то к 2004 году в американских и европейских изданиях заговорили о хакерах и спамерах, как о членах организованных преступных групп, способных принести западной экономике многомиллионные убытки.

Первым тому подтверждением стал компьютерный вирус MyDoom — сетевой червь, который стал самой быстораспространяемой из когда либо зарегистрированных вредоносной компьютерной программой. Хотя настоящий автор вируса так и не был обнаружен, несколько компаний, работающих в области компьютерной безопасности заявили о том, что вирус написан русскими программистами. Версию охотно подхватили СМИ, которые позже опубликовали сведения о многомиллионных потерях, которые нанес вирус мировой экономике.

Также в 2004 году были пойманы, а позже приговорены к длительным срокам и денежным штрафам заключения трое граждан России, Иван Максаков, Александр Петров и Денис Степанов. Они устраивали заказные DDoS-атаки на британские и американские сайты. В результате атак сайты, включая тотализаторы и онлайн-казино потеряли миллионы долларов в виде упущенной выгоды. И снова Россия предстала в западных СМИ в образе страны, которая выращивает особо агрессивных и безжалостных киберпреступников.

Июль 2007 — август 2008: проблема становится серьезнее

К середине 2007 года западные СМИ рассматривали проблему киберпреступности уже в контексте освещения деятельности целых преступных сообществ, работающих в России. В ряде публикаций речь шла о так называемой Российской деловой сети (Russian Business Network, RBN) — специальном хостинге, который не принимал жалобы на содержимое размещенных на нем сайтов. Хостинг был расположен в Санкт-Петербурге и считался крупнейшим ресурсом для распространителей спама, вредоносного программного обеспечения, торговли нелегальными или поддельными товарами (например, фармацевтическими препаратами) и даже детской порнографии. Создателей RBN подозревают также в разработке знаменитой ботсети Storm, предназначение которой до сих пор неизвестно. Также услугами RBN, по сообщениям западных СМИ, пользовалась крупнейшая в мире организация, зарабатывающая на распространении фармацевтического спама, так называемая партнерская программа Glavmed.com, которая значилась в рейтинге Spamhaus.org как проект Canadian Pharmacy и считается крупнейшим спамером в мире.

Начиная с июля 2008 года западную прессу вновь заинтересовала тема российской киберпреступности. На этот раз в связи с кратковременным военным конфликтом между Россией и Грузией. Грузинские власти обвинили Москву — и эта точка зрения активно поддерживалась американскими и европейскими СМИ — в кибератаках на грузинские компьютерные сети. Подобные атаки на компьютерные сети Эстонии уже упоминались в западных СМИ в 2007 году. Выдвигались версии о том, что атаки на Грузию производились с ресурсов RBN. Российское правительство активно опровергало сообщения о том, что им поддерживаются кибератаки на Грузию, однако агрессивная и

пропагандистская позиция западной прессы оставалась неизменной. Уже существующий образ России-родины киберпреступников был успешно развит и дополнен новыми сообщениями, в результате чего вышло, что Россия формирует киберугрозу для всего остального мира и готова воспользоваться своим кибероружием в любое время для достижения политических целей.

Март 2009 — март 2010 года: обеспокоенность приобретает политическую окраску

К концу рассматриваемого периода количество сообщений о российской киберпреступности в абсолютном выражении стало в четыре раза больше, чем в 2000 году. В феврале 2010 года Россия упоминалась в связи с угрозой глобальной эпидемии сетевого червя Conficker, к создателям которого причисляют неизвестных российских программистов, объединенных в западной прессе под коллективным псевдонимом «русские хакеры».

Особое звучание приобрела тема спама, связываемая с организованными преступными группами, состоящими, в основном, из граждан России. Так, например, осенью 2009 года многие западные издания сообщили о том, что почтовые ящики по всему миру завалены спамом, предлагающим лекарства от свиного гриппа, продаваемые через российскую партнерскую программу Glavmed.

Как мы уже отмечали, тема киберпреступности, организуемой российскими спаммерами с целью извлечения прибыли, прочно закрепилась на страницах западных СМИ. Однако к этой теме добавилась и более важная — геополитическая. Россию стали обвинять в государственной поддержке киберпреступников.

Немалое влияние на отношение западной прессы к теме киберпреступности оказало заявление президента США Барака Обамы о намерении создать должность советника по вопросам кибербезопасности и специальное военное подразделение, в обязанности которого входит защита государственных объектов США от кибератак. В конце года на должность советника по кибербезопасности был назначен Говард Шмидт, занимавший ранее пост главного директора по информационной безопасности в компании Microsoft. Это назначение как будто стало сигналом для западной прессы, которая включила сообщения о киберугрозах в повестку дня своих полос, рассказывающих о зарубежной жизни.

В конце 2009 года для обвинения России в ведении кибервойны с Западом нашелся еще один подходящий повод — так называемый Климатгейт. Скандал поистине международного масштаба произошел на ежегодном климатическом саммите в Копенгагене. Переписка ученых, которые сомневаются в том, что деятельность человека негативно влияет на климат, стала доступна широкой общественности, поставив под вопрос само существование проблемы глобального потепления. Западные СМИ

немедленно обвинили во взломе почтовых аккаунтов Россию, которая является одним из крупнейших мировых поставщиков нефти и газа и сильно заинтересована в том, чтобы результаты саммита в Копенгагене не привели к ужесточению международных норм выброса углекислого газа в атмосферу. Любопытно, что никаких доказательств версии о российских хакерах, работающих на правительство, представлено не было. Однако это не мешает крупнейшим западным СМИ при появлении первых признаков заметного киберпреступления немедленно обвинять Россию. Сейчас это происходит уже рефлекторно, так как репутация нашей страны в сфере ответственного сосуществования в информационном обществе сильно подпорчена.

Единственным спасением от навешивания ярлыка главного киберпреступника в мире Россию может спасти только активное противостояние Запада с Китаем, которое, как уже было отмечено, началось в 2007 году. Сейчас это противостояние только усилилось, и уже в начале 2010 года было отмечено крупным конфликтом с крупнейшей интернет-компанией мира — Google. Компания официально сообщила о взломе своих почтовых ящиков в Китае, после чего последовало заявление о том, что Google прекращает деятельность своей поисковой машины на территории Китая по причине жестких требований китайского правительства по фильтрации результатов поиска.

В настоящий момент западные СМИ уже сформировали представление об интернете, как о новом поле битвы для крупнейших стран мира. И на этом поле у США и Европы есть два главных врага — Россия и Китай. Если Россия продолжит сохранит нейтральность своего законодательства в отношении спаммеров и киберпреступников, в обозримом будущем ей будет трудно исправить негативный образ рассадника киберпреступности, не только сформированный западными СМИ, но и активно поддерживаемый реальными преступлениями, которые совершаются гражданами России. Этот образ в не самой отдаленной перспективе может снизить и инвестиционную привлекательность российский интернет- и ИТ-компаний как для западных стратегических, так и частных инвесторов, мнение которых как раз и формируется публикациями в крупных СМИ.