в декабре 2015 г., ибо время и общественное мнение, сформированное фильмами Хайо Зеппельта про допинг и Россию, работало против нашей страны. Поиски путей информационного решения данной кризисной ситуации — это уже тема последующих научных изысканий.

Примечания

[1] См.: http://hajoseppelt.de/2014/12/the-secrets-of-doping-how-russia-makes-its-winners/.

[2] Сайт BBC.18.07.2016 г.

[3] См.: http://www.autentic-distribution.com/en/product/do/detail.html?id=3935; http://hajoseppelt.de/2015/08/doping-top-secret-the-shadowy-world-of-athletics/; https://www.theguardian.com/sport/2016/jun/16/sebastian-coe-moment-of-truth; http://www.bbc.com/sport/athletics/33749208.

[4] См.: http://hajoseppelt.de/2016/03/doping-secret-russias-red-herrings/.

[5] См.: http://www.ardmediathek.de/tv/Sportschau/Doping-Top-Secret-The-Protection-Rack/Das-Erste/Video?bcastId=53524&documentId=39197456; http://www.playthegame.org/news/news-articles/2016/0251_new-claims-further-involve-iaaf-top-in-russian-doping-coverups/.

Лай Линчжи
Санкт-Петербургский гос. ун-т

## Средства информационно-психологической защиты государства от информационных атак сетевых СМИ (на примере Китая)

Как и многие другие страны, существующие в эпоху информационной глобализации, Китай тоже сталкивается с проблемой сетевых атак. В данной статье сделан акцент на средства информационно-психологической защиты государства от информационных атак сетевых СМИ в Китае.

*Ключевые слова:* информационно-психологическая защита, информационная атака, сетевые СМИ.

Lai Lingzhi
St. Petersburg State University

## Means of information-psychological protection of the state against the information attacks of media network (on the example of China)

Like many other countries, coexisting in the era of information globalization, China also faces the problem of network attacks. This article focuses on the means of information-psychological protection of the state against information attacks of network media in China.

*Keywords:* information-psychological protection, information attack, media network.

Сетевая атака — это попытка воздействовать на удаленный компьютер с использованием программных методов. Как правило, целью сетевой атаки является нарушение конфиденциальности данных, т. е. кража информации. Кроме того, сетевые атаки проводятся для получения доступа к чужому компьютеру и последующего изменения файлов, расположенных в нем. Есть несколько типов классификации сетевых атак. Один из них — по *принципу воздействия*. Пассивные сетевые атаки направлены на получение конфиденциальной информации с удаленного компьютера. К таким атакам, например, относится чтение входящих и исходящих сообщений по электронной почте. Что касается активных сетевых атак, то их задачей является не только доступ к тем или иным сведениям, но и их модификации.

Существуют многочисленные объективные факторы появления сетевых атак. В том числе технические возможности создают важную почву для их появления: существует огромное множество различных конфигураций компьютеров, операционных

систем и сетевого оборудования, однако это не становится препятствием для доступа в глобальную сеть. Такая ситуация стала возможной, благодаря универсальному сетевому протоколу TCP/IP, устанавливающему определенные стандарты и правила для передачи данных через Интернет. К сожалению, подобная универсальность привела к тому, что компьютеры, использующие данный протокол, стали уязвимы для внешнего воздействия, а поскольку протокол TCP/IP используется на всех компьютерах, подключенных к Интернету, у злоумышленников нет необходимости разрабатывать индивидуальные средства доступа к чужим машинам[1].

Как и многие другие страны, существующие в эпоху информационной глобализации, Китай тоже сталкивается с проблемой сетевых атак. 22 сентября 2015 г. в Сиэтле председатель КПК Си Цзиньпин выступил с речью об информационной безопасности, где, в частности, сказал: «Мировое сообщество непрестанно критикует Китай за осуществление сетевых атак. Иногда из-за неправильного понимания, иногда из-за нехватки информации и иногда даже из-за недоброго намерения. На самом деле Китай является одной из стран, страдающих от сетевых атак. Китай не будет стоять в стороне от защиты информационной безопасности»[2].

Китай использует несколько видов защиты от сетевых атак. *Регулирование Интернета.* В 2008 г. на первой сессии Всекитайского собрания народных представителей 11 созыва было создано Министерство промышленности и информатизации КНР, отвечающее за регулирование и развитие в стране почтовой связи, Интернета, беспроводной связи, теле- и радиовещания, производства электронных и информационных товаров, индустрии программного обеспечения и развитие информационного общества. Обязанностями данного министерства являются управление коммуникационной отраслью, содействие информатизацию страны, обеспечение и координация государственной информационной безопасности, развитие важнейшего технического оборудования и инноваций, контролирование повседневного функционирования промышленной отрасли,

выработка и осуществление отраслевой планировки, политики и стандарта[3].

За менее чем годовой срок было разработано законодательное поле и 22 февраля было опубликовано одно небольшое извещение о требовании к сайтам. 24 февраля 2009 г. Министерство промышленности и информатизации КНР закрыло доступ к более чем 100 тысячам сайтов, у которых не было соответствующей ISP (Internet Service Provider) — лицензии или же регистрационные данные не совпадали с реальными, были поддельными и т. п. Начиная с 2009 г. в отчетах Минпроминформатизации ежегодно публикуется «Уровень сайтов, взятых в делопроизводство» и «Уровень правдивости регистрационной информации интернет-сайтов»[4].

*Обеспечение персональной информационной безопасности.* В целях обеспечения информационной безопасности страны Государственный Совет КНР призвал ужесточить порядок сбора персональных данных корпорациями и частными компаниями и потребовал от министерств обеспечить безопасность персональных данных при передаче их от одного ведомства другому. В начале 2013 г. китайские власти обратились к частным компаниям с призывом улучшить противодействие хакерам и похитителям персональных данных в Сети. 17 июля 2012 г. Госсовет КНР издал директиву, в которой министерствам настоятельно рекомендуется уменьшить количество каналов, по которым хакеры могут предпринять атаки на то или иное ведомство, а также усилить надзор за доступом к засекреченной информации. Энергетическая и финансовая отрасли, атомные объекты, предприятия, задействованные в космической программе КНР, а также крупные инфраструктурные проекты обязаны будут усиливать меры информационной безопасности и ужесточать контроль за доступом к информации. В соответствии с положениями директивы, основные усилия должны быть направлены на повышение эффективности обнаружения проникновений в системы безопасности и их локализацию, активизацию борьбы с интернет-преступностью и защиту персональных данных миллионов китайских граждан[5].

*Международное сотрудничество.* В эпоху информационного общества информационная безопасность и кибербезопасность стали одной из ключевых вопросов мирового масштаба. И в контексте глобализации решение данных проблем может быть осуществлено в рамках международного сотрудничества. В последние годы международное сообщество уделяет всё больше внимания выработке международных правил, стандартизации поведения в информационном и киберпространстве.

В 2011 г. постоянные представители Китая, России, Таджикистана и Узбекистана при ООН совместно направили послание в адрес генерального секретаря ООН Пан Ги Муна, в котором попросили его распространить на 66-й сессии Генеральной Ассамблеи ООН критерии, совместно составленные этими четырьмя государствами, в качестве официального документа и призвали все страны развернуть дальнейшее обсуждение вопроса защиты информационных атак в рамках ООН, чтобы как можно скорее добиться консенсуса по формализации международных критериев и правил поведения в информационной области и киберпространстве. Данный документ под называнием «Международные критерии поведения для информационной безопасности» является первым сравнительно всеобъемлющим и систематичным документом о международных правилах информационного поведения и кибербезопасности.

В этом документе выдвинут ряд основных принципов по сохранению информационной и кибербезопасности, охватывающей политическую, военную, экономическую, социальную, культурную и техническую сферы. В документе указано, что странам не следует использовать информационные и телекоммуникационные технологии, включая компьютерную сеть, для совершения враждебных и агрессивных актов и создания угроз миру и безопасности на планете; страны имеют обязательства и право защищать свое информационное пространство и киберпространство, а также свои ключевые объекты информационной инфраструктуры и киберинфраструктуры от угроз, вмешательства, нападения и нарушений. Кроме того, в документе говорится о необходимости создать многосторонний, прозрачный и

демократический механизм международного контроля за Интернетом, призванный помочь развивающимся странам в развитии информационных и кибертехнологий, а также наладить сотрудничество в борьбе с киберпреступностью[6].

*Развитие и реконструирование информационной структуры страны.* В целях эффективного противостояния информационным атакам извне и усиления технологических возможностей защиты страны от них, а также с целью соответствия тенденциям мирового развития, Китай предлагает направить усилия на реконструкцию экономической структуры и улучшение информационного потенциала страны[7].

Кроме того, проведение исследований в области информационной безопасности и предложения финансовой и политической поддержки исследований в данной области является немаловажными методами защиты страны от информационных атак в Китае.

*Организации по защите от сетевых атак в Китае.* В данный момент в Китае работают следующие организации, контролирующие Интернет и защищающие от информационных атак: Министерство промышленности и информатизации КНР, курирующее группу интернет-безопасности ЦК КПК в составе Министерства Культуры КНР, департамент интернет-безопасности и защиты Министерства Общественной Безопасности КНР и другие. Ключевую роль играет Департамент интернет-безопасности и защиты министерства Общественной Безопасности КНР, который берет на себя следующие функции :

1. Осуществлять надзор, контроль и управление защитой компьютерной информационной системы.

2. Давать оценку, осуществлять проверку и одобрять в случае необходимости информационную систему.

3. Проводить расследование компьютерных преступлений.

4. Упорядочивать важнейшие инциденты в сфере информационной безопасности.

5. Принимать ответственные меры к предотвращению атак информационных вирусов и вредных данных.

6. Управлять специальными продуктами, отвечающими за информационную безопасность компьютерной системы.

7. Отвечать за подготовку управленческих кадров в сфере информационной безопасности[8].

В Китае уделяют особое внимание управлению веб-сайтами для подростков. Цель — защищать их от информационных и психологических травм, полученных в ходе сетевых атак.

По статистике, подростки составляют большинство интернет-пользователей. В настоящее время в Интернете распространяются различные виды порнографической информации. Учитывая тот факт, что психологически и физически неокрепшие подростки, находящиеся в несовершеннолетнем возрасте, способны к осуществлению преступных деяний, перед государством стоит задача защиты этой категории лиц. Согласно статистическим данным, в настоящее время в мировом масштабе насчитывают примерно 20 тысяч порнографических сайтов, а посещаемость самых популярных из них насчитывает свыше 200 тысяч посещений в день. Они, весьма вероятно, окажут негативное влияние на психологию подростков при отсутствии эффективного регулирования и контроли над этими сайтами[9].

Чтобы создать более позитивный и здоровый онлайн-мир и избежать преступления подростков, необходимо усилить информационный контроль в Интернете. Именно поэтому мы предлагаем следующие рекомендации.

*Во-первых,* активизировать усилия по совершенствованию соответствующего законодательства.

Хотя в законодательстве Китая есть частичные нормы по защите подростков от сетевых атак, но большинство из них не могут удовлетворять реальные потребности в связи с непрерывным развитием сетевых технологий. До сих пор в Китае отсутствует специальный закон, регулирующий доступ подростков к информации. Именно поэтому надо пересмотреть, улучшить и усовершенствовать существующие законы о защите подростков в Сети. И, кроме этого, можно и нужно на законодательном уровне запрещать сетевым компаниям публиковать, воспроизводить или перепечатать негативную информацию, связанную с порнографическим содержаниям, и

информацию, которая угрожает национальной безопасности или которая противоречит культурной традиции и ментальному восприятию народа.

*Во-вторых,* саморегулирование интернет-производителей также является немаловажным фактором. Производители не должны сознательно производить и распространять нездоровые, бескультурные, вредные информационные продукты любой формы; не должны предлагать интернет-игры, показывающие насилие или имеющие порнографическое содержание.

*В-третьих,* усиление медиавоспитания молодёжи, способной заниматься селекцией сетевой информации. Это является одним из самых эффективных способов защиты от воздействий негативной информации.

В 2011 г. из-за рубежа с 47 тысяч иностранных IP-адресов было атаковано 8,9 миллиона компьютеров. Согласно докладу Центра национальной координационной сети реагирования на чрезвычайные ситуации КНР, несмотря на усиленные меры защиты, в последнее время Китай все чаще сталкивается с кибератаками из-за границы[10].

Именно поэтому в Китае принимают усиленные меры по противостоянию сетевым атакам и обеспечению национальной информационной безопасности. Например, в марте 2015 г. Департаментом информации в Интернете были приняты «10 правил аккаунтов», исходя из которых владелец сайта, входящего в перечень, обязан предоставлять реальные данные и должен запрашивать у пользователя подтверждение его личности[11].

Хотя в Китае уже принимаются многочисленные меры защиты от сетевых атак, в стране всё равно нет отдельной конкретной стратегии по ведению борьбы в киберпространстве в связи с неопределённостью и непредсказуемостью сетевых атак. Полагаем, что благодаря техническому развитию и международному сотрудничеству, а также установлению более адекватной политической стратегии в этой области Китай будет способен решать проблему борьбы с сетевыми атаками более эффективно.

Примечания

[1] Что такое сетевая атака. URL: http://www.kakprosto.ru/kak-848505-chto-takoe-setevaya-ataka (Дата обращения 06.02.2017).

[2] Там же.

[3] Хи Цзиньпин: Китай тоже является страной страдающей от сетевых атак. URL: http://news.china.com/focus/xjpfm/zb/ 11174287/20150924/20455223_all.html.

[4] *Ковалёв Г.* Регулирование интернета в Китае. URL: https://geektimes.ru/post/248120/.

[5] Там же.

[6] *Исмаилов Р.* Обеспечение кибербезопасности — китайский опыт ведения виртуальной войны. URL:http://politinform.su/informacionnye-voyny/4697-obespechenie-kiberbezopasnosti-kitayskiy-opyt-vedeniya-virtualnoy-voyny.html.

[7] Китай, Россия, Таджикистан и Узбекистан совместно представили ООН «Международные критерии поведения для информационной безопасности». URL: http://www.russian.people.com.cn/31520/7594385.html.

[8] Государственный информационный центр : расширить инвестиционный обьем, чтобы реконструировать и улучшить модель развития. URL: http://futures.hexun.com/2012-07-13/143530759.html.

[8] URL: http://baike.baidu.com/item/=aladdin.

[9] *Шэн Хонсяо.* Немного о плюсах и минусах социальных сайтов для подростков как причины вызывания преступления и выход к решению существующих проблем. URL: http:// blog.sina.com.cn/s/ blog_12e5b9cdf0102vk4q. html.

[10] *Исмаилов Р.* Указ. соч.

[11] *Ковалёв Г.* Указ. соч.

Г. С. Мельник
Санкт-Петербургский гос. ун-т

## Тактические медиа как протестный ресурс

Тактические массмедиа рассматриваются в одном ряду с такими видами новой сетевой журналистики, как гражданская, соци-