УДК 070.1

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СМИ В УСЛОВИЯХ КИБЕРВОЙНЫ

© 2012 В.А. Голуб

Воронежский государственный университет

Поступила в редакцию 13 апреля 2012 года

Аннотация: *Средства массовой информации являются не только «оружием» в информационной войне, но и одной из основных целей для кибератак противника, стремящегося достичь превосходства в информационном пространстве, что требует принятия самых серьезных мер по обеспечению информационной безопасности СМИ.*

Ключевые слова: *СМИ, информационная безопасность, информационная война, кибервойна.*

Abstract: *Mass-media is not only a weapon in the information war, but one of the main purpose for the ciber-attack of the enemy, who seek to score superiority in the information space. It demand to attempt the most serious activity for information security ensuring.*

Key words: *mass-media, information security, information war, ciber war.*

Средства массовой информации уже давно стали важнейшим инструментом усиления позиций одной из сторон в любом сколь-нибудь серьезном политическом, экономическом или военном конфликте. СМИ как оружие, используемое в информационной войне, призваны обеспечить достижение информационного превосходства в конфликтной ситуации.

Впервые термин «информационная война» был использован в 1976 году Томасом Роном в отчете «Системы оружия и информационная война», а официально употреблен в 1992 году в директиве министра обороны США. В последние годы это понятие приобретает все более широкий смысл. «Объединенная доктрина информационных операций», введенная в действие в 1998 году министерством обороны США определяет информационную войну как «комплексное воздействие (совокупность информационных операций) на систему государственного и военного управления противника, на его военно-политическое руководство с целью принятия им уже в мирное время благоприятных для страны-инициатора информационного воздействия решений и полной парализации инфраструктуры управления противника в ходе конфликта» [1]. По опубликованным данным, более чем в 120 странах мира разрабатываются методы информационно-компьютерного воздействия на информационный ресурс потенциального противника [2].

Наиболее часто выделяют два значения термина «информационная война»: как воздействие на гражданское население и (или) военнослужащих другого государства путём распространения определённой информации [3] и как целенаправленные действия, предпринятые для достижения превосходства в информационном и в военно-политическом противоборстве путем нанесения ущерба информации, информационным процессам и информационным системам противника при одновременной защите собственной информации, информационных процессов и информационных систем [4]. Средства массовой информации самым активным образом могут быть задействованы для решения задач информационной войны, что и наблюдается на практике последние 20 лет при освещении военных конфликтов в Панаме (1989 год), на Гаити (1994 год), во время операции «Буря в пустыне», в Югославии (1999 год), в Афганистане (2002 год) и Ираке (с 2003 года).

Особенностью информационной войны является то, что она не предполагает проведение традиционных боевых операций. Современные информационные «боевые действия» ведутся в киберпространстве глобальной сети Интернет, что объясняется, прежде всего, простотой получения и общедоступностью информации, распространяемой в сети. В условиях межгосударственного конфликта не только публикации печатных СМИ, но и телевизионные и радиопередачи одной из конфликтующих сторон, становятся недоступны населению другой стороны, даже если в обычных условиях этого не наблюдалось, а сетевой доступ в Интернет в большинстве случаев остается работоспо-

собным. Под кибервойной можно понимать целенаправленные сетевые атаки в Интернете, направленные на взлом, блокирование или иное воздействие на компьютерные системы и сетевые ресурсы противника с целью нарушения их работоспособности.

В военном конфликте СМИ занимают особое место, что определяет и их положение как одной из основных целей в кибервойне. Масс-медиа в информационном противостоянии выполняют функции информационного обеспечения, формирования и трансформации политических, идеологических и геополитических взглядов общества, психологического воздействия и дезинформации противной стороны. Важной задачей СМИ при освещении вооруженного противостояния является создание образа врага и дискредитация противника, а также формирование в общественном сознании положительного образа своих вооруженных сил и органов управления, проведение идеи справедливой войны. Сетевые атаки на интернет-ресурсы СМИ, как правило, имеют целью достижение преимущества в информационном противоборстве путем деструктивного воздействия на системы управления и принятия решений путем осуществления психологических операций, реализации мероприятий по оперативной и стратегической маскировке оперативных действий и дезинформации [5]. Для снижения эффективности информационного воздействия, осуществляемого противником, возможны различные контрмеры, среди которых выделяются хакерские по своей сути атаки, призванные на техническом уровне нейтрализовать интернет-СМИ, что и есть проявление кибервойны, как составляющей войны информационной.

Характерной особенностью информационных войн последнего времени стало широкое использование сетевых атак на интернет-ресурсы противной стороны. Такие нападения могут быть весьма разнообразны по технологии проведения и решаемым тактическим задачам (полное или частичное блокирование атакуемого сайта, уничтожение его контента, хищение конфиденциальной информации и т.п.), но конечной целью всегда будет нейтрализация интернет-медиа противника для достижения доминирующего положения в информационном пространстве. Самым распространенным, но далеко не единственным, способом воздействия на сайты интернет-медиа является проведения распределенных атак на отказ в обслуживании (DDoS-атаки), когда сервер, предоставляющий медиа-ресурсу услуги хостинга, не выдерживает генерируемого хакерской сетью интенсивного потока запросов на обслуживание и оказывается заблокированным.

Одним из самых показательных примеров интернет-атак в условиях ведения информационной войны является ситуация, сложившаяся во время грузино-российского вооруженного конфликта в августе 2008 года. Сразу после начала боевых действий на территории Южной Осетии 8 августа были атакованы югоосетинские СМИ – сайт информационного агентства «Осинформ» и сайт осетинского радио и телевидения. Затем последовали нападения на грузинские интернет-ресурсы: был взломан сайт МИД Грузии и на нем был размещен фотоколлаж из снимков Гитлера и Саакашвили. Также были атакованы сайт «Грузия online», сайт агентства «Новости-Грузия» и сайт президента Грузии М. Саакашвили, а грузинские онлайн-СМИ civil.ge и «Свободная Грузия» были заблокированы вследствие DDoS-атаки. Через 3 дня были выведены их строя сайт РИА Новости и сайт англоязычного телеканала Russia Today [6].

Приведенные примеры показывают, что одним из показателей готовности СМИ к информационной войне в киберпространстве является устойчивость их интернет-ресурсов к сетевым нападениям. Это обусловливает повышенные требования к специалистам, задействованным в создании и обеспечении функционирования информационно-телекоммуникационных систем СМИ, а также к журналистам, которые работают с сетевым медиа-ресурсом. Последнее положение обосновывается тем, что ошибки и неквалифицированные действия журналистов-пользователей компьютеров могут способствовать созданию предпосылок для реализации угроз информационной безопасности СМИ. Причем далеко не всегда существует возможность нейтрализации ошибочных действий методами системного администрирования или с помощью программных средств защиты.

Нападения на СМИ в Интернете могут осуществляться не только усилиями государственных структур, но и отдельных лиц, в частности, из патриотических побуждений. Такая ситуация наблюдалась и во время уже упомянутого Российско-Грузинского вооруженного конфликта 2008 года. Весьма серьезную опасность представляет «кибернетизация» терроризма. По мнению Т. Гусельниковой «масс-медиа становятся перспективной мишенью для «революционеров XXI века». Эксперты утверждают: если традиционный терроризм не угрожал обществу как целостной системе, то высокотехнологический терроризм новой эпохи вполне может спровоцировать кризис государства с развитой инфраструктурой информационного общества» [7]. Необходимо подчеркнуть, что СМИ являются одной из целей кибер-преступников, причем вероятность нападения на то или иное издание

будет тем больше, чем большее влияние на аудиторию оно оказывает.

Сегодня эффективность кибервойн признана на государственном уровне. По сообщениям СМИ целый ряд государств (США, Россия, Китай, КНДР, Израиль и др.) сформировали специальные структуры для ведения «боевых» действий в киберпространстве и для защиты от таких действий. Так, в США для противостояния информационным угрозам и отражения атак на инфраструктуру страны создано специальное командование и в решении этих задач задействовано примерно 16 тысяч высококвалифицированных специалистов, в то время как в России – порядка тысячи человек [8]. Совершенно очевидно, что эти ресурсы не ориентированы на решение проблем информационной безопасности средств массовой информации, а значит, СМИ должны решать проблемы безопасности самостоятельно. Директор американского Управления по борьбе с компьютерными преступлениями Скотт Борг считает: «Это новая эра. Теперь все политические и военные конфликты будут иметь компьютерный компонент» [9], а значит, будет постоянно возрастать вероятность того, что вовлеченные в информационное противостояние СМИ будут подвергаться все большей опасности.

Таким образом, в условиях конфликтной ситуации интернет-медиа подвержены повышенному риску сетевых атак, результатом которых может быть полное или частичное нарушение их работы. Для предотвращения таких ситуаций необходим ряд превентивных организационных и технических мероприятий, направленных на обеспечение информационной безопасности СМИ.

ЛИТЕРАТУРА:

1. Концепция сетевой войны / Пси-фактор. – (http://psyfactor.org/psyops/webwar.htm).

2. Ахмедова Афаг. Безопасность в информационный век // It2b – Технологии разведки для бизнеса. – (http://it2b.ru/blog/infowars/709.html).

3. Манойло А.В. Информационно-психологическая война : факторы, определяющие формат современного вооруженного конфликта / А.В. Манойло // Пси-фактор. – (http://psyfactor.org/lib/psywar35.htm).

4. Глоссарий. – (http://www.glossary.ru/).

5. Гриняев С.Н. Информационная война: история, день сегодняшний и перспектива / С.Н. Гриняев // Агентура.ру. – (http://www.agentura.ru/equipment/psih/info/war/).

6. Федина Ольга. Принуждение к миру в Сети. Война в Интернете велась не менее ожесточенно, чем в реальной жизни / Ольга Федина // Компромат.Ru. – (http://www.compromat.ru/page_23174.htm).

7. Гусельникова Таис. Информационная война / Таис Гусельникова // Персональный сайт журналиста Таис Гусельниковой. – (http://www.tais-world.com/articles/information-war).

8. Верный Руслан. Третья мировая уже началась – в Интернете / Руслан Верный // «Соль». – (http://www.saltt.ru/node/7014).

9. Американские эксперты встревожены атаками российских хакеров на грузинские сайты. / SecurityLab. – (http://www.securitylab.ru/news/358219.php).

Голуб В.А.
Кандидат технических наук, доцент кафедры рекламы и дизайна факультета журналистики Воронежского государственного университета.
E–mail: v.a.golub@yandex.ru, vgol@list.ru.

Golub V.A.
Voronezh State University, Candidate of Technical Sciences, Associate Professor, Department of Advertisement and Design.