УДК 070.13

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СМИ КАК ФАКТОР ОБЕСПЕЧЕНИЯ СВОБОДЫ СЛОВА

© 2010 В.А. Голуб

Воронежский государственный университет

Поступила в редакцию 14 сентября 2010 года

Аннотация: *В статье рассматривается влияние информационной безопасности СМИ на возможность реализации свободы слова. Показано, что недочеты в обеспечении информационной безопасности СМИ делают реальную свобода слова практически недостижимой.*

Ключевые слова: *свобода слова, информационная безопасность, средства массовой информации.*

Abstract: *In clause influence of information security of mass-media on an opportunity of realization of a freedom of speech is considered. It is shown, that mass-media information security organization defects do real a freedom of speech practically unattainable.*

Key words: *freedom of speech, information security, mass-media.*

Свобода слова является важнейшим достижением демократии, без которого невозможно развитие демократического общества. Свободная пресса и электронные СМИ представляются гарантами защиты общества от стагнации и регресса, основными инструментами формировании и информирования гражданского общества. Законодательное обеспечение деятельности СМИ является основным фактором обеспечения их свободы. Важным является и экономическая независимость СМИ. Но каким бы совершенным ни было законодательство, какими бы материальными и финансовыми ресурсами ни обладали печатные и электронные средства массовой коммуникации, имеется целый ряд факторов, которые, не имея, на первый взгляд, прямого отношения к обеспечению свободы СМИ, тем не менее, могут выступать как ограничители этой свободы. К таким факторам относятся, в частности, уязвимости в системе обеспечения информационной безопасности средств массовой коммуникации.

В условиях, когда большая часть технологических процессов функционирования любой редакции компьютеризирована и предполагает широкое использование современных цифровых телекоммуникационных средств, сбои в работе систем обработки и передачи информации могут приводить к крайне негативным последствиям, вплоть до полного блокирования деятельности СМИ. Особенно уязвимыми являются электронные средства массовой информации. Так, предумышленное нарушение связи с корреспондентом во время прямого телевизионного или радиоэфира, может сорвать передачу, но еще более опасным является длительное блокирование каналов связи, по которым важная информация должна быть срочно передана в редакцию. Такая ситуация по сути своей означает, что осуществляется препятствование законной деятельности СМИ по информированию общества, т.е. ограничения свободы слова.

Слежка за журналистами и прослушивание их переговоров в ряде случаев также могут рассматриваться как непосредственное препятствование их профессиональной деятельности, либо факторы, создающие предпосылки для этого. Слежка и прослушивание переговоров дают возможность определить источники информации, что является

нарушением их конфиденциальности и может быть направлено на недопущение получения необходимых сведений средствами массовой информации, а это уже – непосредственное нарушение принципов обеспечения свободы слова. Важность этого обстоятельства отмечается и в Европейской хартии свободы прессы, одной из предпосылок разработки которой явилось признание редакторами и журналистами ряда стран того, что для полноценного решения ими профессиональных задач им не хватает имеющихся демократических свобод. Подписание Хартии состоялось 25 мая 2009 года в Гамбурге (ФРГ), причем текст Хартии размещен в Интернете и доступен для подписания каждому журналисту. В 10 статьях хартии сформулированы принципы свободы СМИ от вмешательства правительства, недопустимости цензуры, прослушивания и обыска редакций, а также необходимости беспрепятственного доступа для журналистов ко всем местным и зарубежным источникам информации [1]. Статья 4 Европейской хартии свободы прессы гласит: «Защита источников информации журналистов должна строго соблюдаться. Обыск новостных редакций и других помещений для журналистов, слежка и прослушивание переговоров журналистов с целью определения источников информации или посягательства на конфиденциальность неприемлемы». Требования по защите конфиденциальных сведений содержатся и в Законе Российской Федерации «О средствах массовой информации», статья 41 которого декларирует обязанность редакции сохранять в тайне источник информации и лиц, предоставивших сведения с условием неразглашения их имени (за исключением случая, когда соответствующее требование поступило от суда в связи с находящимся в его производстве делом).

Ясно, что заявленная в 4-й статье Хартии неприемлемость слежки за журналистами и прослушивания их разговоров является декларацией до тех пор, пока не получает законодательного подкрепления при обязательном выполнении требований закона. При этом следует подчеркнуть, что даже самое совершенное законодательство и стоящие на его страже четко работающие правоохранительная и судебная системы не могут гарантировать, что нарушений закона не будет. В этой связи следует признать важным и действенным условием обеспечения принципов действительной свободы СМИ и профессиональной деятельности журналистов реализацию требований информационной безопасности. Важным является то, что эти вопросы должны решаться прежде всего самими редакциями, причем крайне важным является достаточный уровень подготовки сотрудников в этой области. Повсеместно принятая практика (и, в принципе, совершенно разумная) состоит в том, что все вопросы информационной безопасности отдаются на откуп компьютерщикам, в предположении, что они сами знают как следует заниматься защитой информации и грамотно сделают свою работу. К сожалению, сегодняшние реалии таковы, что даже работающие в различных СМИ профессионалы, занимающиеся обслуживанием компьютеров и компьютерных сетей, разрабатывающие интернет-сайты и решающие иные вопросы, связанные с использованием компьютерной техники, далеко не всегда хорошо владеют вопросами обеспечения информационной безопасности с учетом особенностей функционирования СМИ.

Самыми молодыми и перспективными среди средств массовой коммуникации являются интернет-издания. Интернет-медиа наиболее широко из всех СМИ используют современные информационные и телекоммуникационные технологии. Но, к сожалению, компьютерные сети относятся к числу систем, наиболее уязвимых с точки зрения защиты информации, т.к. помимо всех тех угроз, которые возможны для печатных и электронных СМИ, интернет-ресурсы подвержены дополнительным очень серьезным угрозам. Проведение успешных сетевых атак на серверы, на которых размещены интернет-издания, способны блокировать их на длительное время, вплоть до полного прекращения их деятельности.

Рассмотрим несколько примеров.

В 2007 году массированной DDoS-атаке подвергся сайт газеты «Коммерсант». По мнению главного редактора сайта Павла Черникова атака могла быть следствием публикации стенограммы допроса Бориса Березовского по делу Александра Литвиненко [2]. Днем раньше был атакован сервер радиостанции «Эхо Москвы», работоспособность которого была нарушена на несколько дней.

По сообщению от 15 сентября 2009 года в результате хакерских атак была полностью уничтожена одесская интернет-газета Odessa Daily [3]. Используя технологию распределенных атак на отказ в обслуживании (DDoS-атаки), осуществляемых с компьютеров, расположенных не только на территории Украины, но и других стран, постоянно, начиная с 7 сентября, злоумышленники добились ликвидации интернет-издания, т.к. восстановить утерянные в результате атаки данные, как следует из слов главного редактора газеты, оказалось невозможным. Кстати, эта информация позволяет сделать вывод, что имелся целый комплекс недоработок в области обеспечения информационной безопасности издания, не только недостаточной оказалась устойчивость сервера к атакам на отказ в обслуживании, но также, по-видимому, в редакции газеты не уделялось

должного внимания резервному копированию данных, если бы это было не так, то по окончании DDoS-атак было бы возможным восстановить основной массив данных.

В Казахстане наблюдались серьезные атаки на сайты отдельных средств массовой информации, интернет-изданий, общественных организаций и политических партий: «Зона.Kz», «Гео.Kz», «Республика.Kz», причем в отдельных случаях защита сайтов не выдерживала и сайты оказывались заблокированными. Это стало поводом для обращения лидеров пяти партий Казахстана к генеральному прокурору с просьбой защитить независимые сайты, Интернет-порталы от «информационного терроризма» и привлечь виновных к ответственности [4]. В связи сетевыми нападениями на интернет-издания председатель правления Союза журналистов Казахстана Сейтказы Матаев отметил, что впервые в Казахстане появился такой термин как «виртуальный терроризм» [5].

Кибератаки на уничтожение в течение длительного времени ведутся против делового обозрения «Республика», представленного двумя веб-сайтами: «Информационно-аналитическим порталом РЕСПУБЛИКА» (зарегистрировано как средство массовой информации в Российской Федерации) и электронной копией еженедельной газеты «РЕСПУБЛИКА – деловое обозрение. Дубль-2» – «Интернет-газета» (поставлена на учет в Республике Казахстан). С сентября 2008 года указанные сайты стали подвергаться сетевым атакам, что вынудило многократно менять предлагающих хостинг провайдеров различных стран, а также вызывало серьезные затруднения в работе изданий. В феврале 2009 года после мощных DDoS-атак, продолжавшиеся в течение двух недель, сайты издания сначала были недоступны, а затем выведены из строя. Очередная смена провайдера не дала эффекта, в силу невозможности противостоять резко увеличивающим трафик атакам очередной провайдер отключил IP-адрес сервера. По сообщению от 7 октября 2009 года, веб-ресурсы издания в течение года подвергались всем видам известных сетевых атак с целью прервать их деятельность, причем очевидно, что атаки носили заказной характер, так как они усиливались в моменты выхода новых материалов издания. Все увеличивающаяся мощность атак позволяет предположить, что конечной их целью является полное уничтожение Интернет-ресурсов, чтобы ни один провайдер не согласился расположить их у себя [6].

Интернет-атаки в ряде случаев могут использоваться для достижения определенных политических целей, например, для того, чтобы помешать оппозиционным СМИ представлять события в соответствии со своими взглядами, что можно трактовать как попытку внедрения в медиапространство для установления своего рода информационных фильтров. Так, осенью 2009 года состоялись хакерские атаки на оппозиционные к действующей власти украинские интернет-издания. Так, когда происходили кровавые события на Одесском рынке «Северный», интернет-изданиям «Ревизору» и «Таймеру», а также сайту телекомпании «АТВ» кто-то целенаправленно мешал оперативно освещать происходящие события, позже атаке подверглось издание «Однако-Украина» [7].

Ночью 1 октября 2009 года сайт российского информационного агентства «Новый Регион», публикующего резкие материалы о политической ситуации на Украине, подвергся мощной DDoS-атаке. Атака оказалась настолько сильной, что создала проблемы не только для московского хостера сайта, но вышла на уровень канала передачи данных и площадки магистрального провайдера «Ростелеком». Атака, направленная не на уязвимость программного обеспечения, установленного на сервере, а на канал передачи данных, создала проблемы с доступом для многих московских хостеров и сайтов использующих этот канал «Ростелекома» [8].

Десятиминутная хакерская атака на сайт газеты «Московский комсомолец», проведенная 3 декабря 2009 года, привела к практически полному уничтожению сайта [9]. По словам главного редактора газеты Павла Гусева, оказались уничтожены фото- и видеоматериалы, утраченными оказались результаты нескольких лет работы по созданию интернета в онлайновом режиме. Хакерская атака привела и к серьезным финансовым потерям, обусловленным, в частности, возникшими проблемами с рекламодателями [10]. Характерно, что в результате кибератаки была уничтожена и система безопасности, предназначенная для защиты сайта от нападений [11]. Судя по тому, что представителями «Московского комсомольца» отмечалась утеря значительного количества материалов, можно предположить, что и в этом случае резервное копирование данных должным образом не выполнялось, что категорически недопустимо.

Еще одно громкое виртуальное нападение на Интернет-ресурс СМИ также относится к 2009 году – в день десятилетия Интернет-издания «Газета.ру» ее сайт подвергся серьезной хакерской DDoS-атаке, что привело к его временной недоступности [12].

Приведенные примеры показывают, что не обеспечить если должным образом информационную безопасность СМИ, то вести речь о реальной свободе слова просто некорректно. Важнейшими факторами, определяющими уровень ущерба от

кибернападений, являются недооценка уровня возможных угроз информационной безопасности средств массовой коммуникации, а также ошибки лиц разрабатывающих и эксплуатирующих системы безопасности СМИ.

В современных условиях не представляет сложности организовать действия по проведению слежки за журналистами, не допустить передачу и опубликование определенного материала, заблокировать Интернет-ресурс и, в некоторых случаях, даже повредить или уничтожить информационные ресурсы того или иного СМИ. Для этого необходимо обладать лишь определенными финансовыми или административными ресурсами. Особенностью преступлений в области высоких технологий является то, что найти преступников часто бывает крайне сложно. Во многих случаях как исполнители, так и организаторы и заказчики преступлений остаются неизвестными и безнаказанными. Недооценка важности обеспечения информационной безопасности средств массовой информации их учредителями, руководителями, сотрудниками, экономия материальных и финансовых ресурсов за счет систем безопасности и обучения персонала лишь облегчают преступникам их задачу. В этих условиях декларируемая законами свобода слова оказывается практически недостижимой.

ЛИТЕРАТУРА

1. Алексеева А. Отныне – свободны! / А. Алексеева. – (http://www.pressing.spb.ru/1/78083).

2. Сайт «Коммерсанта» подвергся DDoS-атаке / Грани.ру. – (http://www.grani.ru/society/Media/m.121500.html).

3. Хакеры уничтожили одесское Интернет-издание. – (http://donbass.ua/news/technology/security/2009/09/15/hakery-unichtozhili-odesskoe-internet-izdanie.html).

4. Мурзалинова-Яковлева С. DDOS атаки способствуют принятию «Интернет» закона в Казахстане / С. Мурзалинова-Яковлева. – (http://www.antiddos.org/index.php/the-news/1-latest-news/126-ddos----qq---), (http://www.logycom.kz/news/newsline/2009/218).

5. Наталья Кунина. Казахстанские интернет-издания атакуют хакеры / Наталья Кунина. – (http://www.ktk.kz/art/?id=3209).

6. Портал «Республика» – ни шагу назад. – (http://www.zakon.kz/149277-portal-respublika-rasskazal-o-ddos.html).

7. Нас атакуют!!! В Украине продолжаются хакерские атаки на оппозиционные интернет-издания. – (http://www.pressing.spb.ru/1/79535/).

8. Заказчиком кибератаки на РИА «Новый Регион» является один из украинских политиков. – (http://www.nr2.ru/moskow/251566.html).

9. Информационное сообщение по поводу кибератаки на сайт «Московского Комсомольца». – (http://www.mk.ru/).

10. Сайт газеты «Московский комсомолец» хакеры взломали с южнокорейского сервера. – (http://synews.ru/russia/2299-cajjt-gazety-moskovskijj-komsomolec-khakery.html).

11. Хакерская атака уничтожила сайт газеты «Московский комсомолец». – (http://www.24news.ru/news/technology/42603383s.html).

12. В день десятилетия хакеры атаковали сайт Интернет-издания «Газета.ру». – (http://www.pressing.spb.ru/1/79328/).

Голуб В.А.
Воронежский государственный университет.
Доцент кафедры рекламы и дизайна, кандидат технических наук.
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.