УДК 070.4

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СМИ И РЕДАКЦИОННЫЙ МЕНЕДЖМЕНТ

© 2011 В.А. Голуб

Воронежский государственный университет

Поступила в редакцию 4 июня 2011 года

Аннотация: *В статье обосновывается, что обеспечение информационной безопасности СМИ является одной из важных задач управления деятельностью редакции. Рассматриваются основные принципы редакционного менеджмента с позиций необходимости обеспечения информационной безопасности.*

Ключевые слова: *журналистика, редакционный менеджмент, информационная безопасность, средства массовой информации.*

Abstract: *Information security of mass-media as an important task of editorial management is substantiated in the article. The main principles of editorial management, taking into account information security ensuring, is considered.*

Key words: *journalism, editorial management, information security, mass-media.*

Редакционный менеджмент обычно рассматривается как деятельность, связанная, в первую очередь, с экономическим управлением редакцией или компанией. Проблема состоит, в частности, в том, что управление работой редакции анализируется в отрыве от крайне опасных тенденций роста угроз информационной безопасности СМИ, в то время как реализация этих угроз способна приводить к серьезным финансовым и репутационным потерям. Без учета необходимости обеспечения информационной безопасности невозможно говорить и о полномасштабном решении основных задач менеджмента и об оптимизации работы редакционного коллектива как в творческом, так и в финансовом плане.

Информационная безопасность является одним из важнейших факторов, определяющих стабильность функционирования средства массовой информации и минимизацию возможных потерь вследствие разного рода эксцессов, обусловленных возможной реализацией угроз информации.

К числу основных принципов редакционной деятельности относят прибыльность издания и обеспечение его конкурентоспособности путем решения следующих задач [1]:

1) оптимизация размеров, состава и структуры коллектива редакции или компании (кадровая политика);

2) оптимизация управления коллективом и организации его работы, включающая регламентацию и организацию работы сотрудников (организационная деятельность);

3) оптимизация результатов этой работы – самого издания, его структуры, модели, системы публикаций и др. (оптимизация результатов).

Рассмотрим эти принципы с позиций необходимости обеспечения информационной безопасности.

Кадровая политика. На сегодняшний день работоспособность компьютерной техники редакции поддерживается либо постоянно работающими в штате редакции системными администраторами, либо привлекаемыми по мере необходимости специалистами-компьютерщиками из других организаций, либо, что характерно для небольших редакций, самими журналистами или другими штатными сотрудниками, которые не являются специалистами в области компью-

терной техники и сетевых технологий. Последний вариант самый экономный и самый опасный.

Условно можно говорить о двух направлениях кадровой политики, исходя из задач обеспечения информационной безопасности СМИ.

Во-первых, подбор высококвалифицированных сотрудников, поддерживающих функционирование компьютерных и информационно-телекоммуникационных систем редакции, которые должны хорошо владеть вопросами обеспечения информационной безопасности. Во-вторых, забота о том, чтобы все сотрудники, работающие с редакционными информационными системами (а такими системами являются, например, компьютеры журналистов, верстальщиков, аппаратура цифровой связи и др.) обладали необходимыми знаниями и навыками по грамотной и безопасной работе с компьютерным и телекоммуникационным оборудованием.

Что касается первого направления, то следует отметить, что существует острый дефицит квалифицированных специалистов-компьютерщиков, хорошо разбирающихся в вопросах информационной безопасности. Кроме того, такие специалисты, как правило, требуют очень высокой оплаты, что далеко не всегда устраивает руководителей, решающих кадровые вопросы. При этом недостаточно грамотный компьютерщик, а таковых подавляющее большинство, просто опасен для организации. Системный администратор имеет полный доступ к компьютерной системе, поэтому его неграмотные, ошибочные действия (или отсутствие необходимых действий) могут иметь самые серьезные негативные последствия.

Относительно второго направления следует отметить, что на сегодняшний день уровень подготовки в области информационной безопасности даже профессионалов-программистов часто весьма низок. Ситуация тем более тревожная, когда речь идет о представителях гуманитарных профессий. Журналистика сегодня самым активным образом использует современные информационные технологии. Это приводит к изменению профессиональных требований, предъявляемых к журналисту. Сегодня журналист должен быть не просто грамотным пользователем компьютерной техники, но и обладать культурой работы с информацией, обязательной составляющей которой является знание основ защиты информации и умение применять эти знания на практике. Пока проблема профессиональной подготовки сотрудников СМИ как пользователей, владеющих в требуемой степени навыками защиты информации, далека от своего разрешения. Между тем, очевидно, что только силами системных администраторов и специалистов-компьютерщиков невозможно решить задачу обеспечения информационной безопасности. Примитивные ошибки в организации парольной защиты, пользовании электронной почтой, работы в Интернете или защите от вредоносного программного обеспечения могут повлечь печальные последствия не только для самого пользователя, но и для организации, в которой он работает, особенно, если компьютеры объединены в корпоративную локальную сеть.

В связи с этим, представляется необходимым организация процесса постоянного повышения квалификации сотрудников редакции в области информационной безопасности, что можно считать одной из важных задач редакционного менеджмента. Причем обучение должно быть действительно постоянным, так как ежедневно появляются новые, ранее не существовавшие виды угроз информационной безопасности, и необходимо знать, как им противодействовать.

Организационная деятельность. Организационной основой обеспечения информационной безопасности редакции, а значит, и важнейшей составляющей управленческой деятельности, является политика безопасности, суть которой в нашем случае можно определить как набор правил разграничения доступа к различным информационным ресурсам организации. Редакционная политика информационной безопасности не может ориентироваться только на профессионалов-компьютерщиков, тем более что в стремлении к сокращению расходов соответствующие должности штатным расписанием небольших редакций часто даже не предусматриваются. Необходимо в обязательном порядке предусматривать регламентацию действий всех пользователей редакционной информационно-телекоммуникационной системы. Это связано с тем, что ряд проблем, связанных как с сохранностью информации, так и с работоспособностью информационно-телекоммуникационных ресурсов редакции, невозможно обеспечить только программно-аппаратными средствами и администрированием. Всегда будет зависимость от того, насколько квалифицированы действия пользователей этих средств, даже если пользователи не обладают правами администраторов.

Управление работой редакции в обязательном порядке должно учитывать необходимость значительных финансовых затрат на обеспечение информационной безопасности. Это затраты на аппаратные и программные средства защиты, на оплату работы специалистов-компьютерщиков или системных администраторов, хорошо разбирающихся в вопросах защиты информации, а также на обучение сотрудников редакции грамотной и безопасной работе с информацией и информационными ресурсами и др. Любые недоработки в сфере обеспечения информационной безопасности чреваты серьезными финансовыми

потерями. Особенно велики потери могут быть, когда речь идет об интернет-изданиях, наиболее подверженных разнообразным атакам и наиболее уязвимым по сравнению с другими СМИ.

В подтверждение этого тезиса рассмотрим несколько примеров.

В первых числах апреля 2011 года с сотен тысяч компьютеров, объединенных в бот-сеть, осуществлялись DDoS-атаки на сайт «Новой газеты», сайт проекта «РосПил» Алексея Навального и Живой Журнал (Livejournal). В результате носивших явно заказной характер кибератак, для организации которых был написан специальных вирус, в течение длительного времени был заблокирован сайт «Новой газеты» и были сорваны организованные этим изданием выборы в Сетевой парламент Рунета [5, 9, 10, 12].

В марте, также вследствие распределенной атаки на отказ в обслуживании, временно была прекращена сетевая активность газеты «Быстрый нейтрон» [4].

В начале января 2011 года DDoS-атакой был заблокирован сайт информационного агентства «Хакасия» [6].

В начале декабря, за сутки до запуска новой версии сайта, хакеры взломали веб-ресурс газеты «Московский комсомолец». При этом было уничтожено все его содержимое, включая редакторский интерфейс и архив за все годы существования сайта [8].

17 декабря успешная хакерская атака была совершена на сайт ежедневной деловой газеты «Ведомости» [7, 15].

В октябре 2010 года мишенью кибер-преступников стала популярная московская интернет-газета The Moscow-post.ru, атакованная с 30000 компьютеров [2].

Сайт известного информационного агентства URA.ru 7 сентября был выведен из строя из-за DDOS атаки. Руководители издания связывают это с острой критикой со стороны агентства действий губернатора А. Мишарина по «продавливанию» института сити-менеджеров в Свердловской области [3].

Не лучше обстоят дела и в других странах. Например, на Украине 24 марта 2011 года мощной DDOS-атаке подвергся портал гражданской журналистики RT.KORR, а затем интернет-издание «Спротив» [17].

В Молдове в начале марта кибератакам подверглось интернет-издание «Коммерсант.мд» [16].

В апреле был неработоспособен сайт Агентства международной информации Trend, вследствие того, что злоумышленники внедрили в программное обеспечение сайта вредоносный java-код, в результате чего вход на сайт агентства блокировался с браузеров Google Chrome и Mozilla Firefox [13, 14].

Как следует из приведенных примеров, современные технические возможности позволяют блокировать работу практически любого интернет-медиа. Очевидно, что ущерб от действий злоумышленников в таких случаях может быть весьма велик. В этой связи серьезной статьей расходов для интернет-медиа может стать необходимость оплаты такого хостига сайта, который позволял бы выдержать интенсивные DDoS-атаки и, тем самым, сохранить работоспособность сайта в критической ситуации.

Здесь стоит также отметить и еще один аспект проблемы информационной безопасности СМИ – возможное нарушение, причем заведомо безнаказанное, основных принципов свободы слова, в то время как законодательно-правовое обеспечение свободы СМИ может быть представлено на достаточно высоком уровне.

Согласно анализу информационных угроз в первом квартале 2011 года, опубликованному «Лабораторией Касперского», фиксируется серьезное увеличение количества атак на различные организации. Также выявляется тенденция переноса деятельности профессиональных преступников, оперирующих в киберпространстве, с домашних компьютеров на взлом корпоративных информационных ресурсов. Причем речь идет не только об обычных DDoS-атаках, которые на некоторое время блокируют интернет-ресурсы компаний, но также о взломе корпоративных серверов с целью похищения информации [11]. В последнее время наблюдается изменение целей преступников, атакующих корпоративные ресурсы, – все чаще их действия направлены не на прямое получение прибыли, а на удар по репутации фирмы. Например, получив доступ к конфиденциальной информации американской компании HBGary, занимающейся компьютерной безопасностью, злоумышленники выложили данные в открытый доступ, в то время как обычно информацию крадут с целью материального обогащения путем ее последующей перепродажи или шантажа, основанного на требовании выкупа за нераспространение полученных сведений.

Специалистами «Лабораторией Касперского» прогнозируется и увеличение количества атак на социальные сети и блоги, информации в которых люди зачастую доверяют не меньше, чем официальным СМИ.

Еще одной важной и весьма опасной тенденцией развития информационных угроз – резкий рост вредоносных приложений («вирусов») как для компьютеров, так и для мобильных устройств. В последнее время смартфоны, коммуникаторы и другая мобильная цифровая техника все чаще используется для хранения и передачи ценной информации, причем не только личной, но и корпо-

ративной. При этом, как указывается в упомянутом отчете, сотрудники компаний относятся к защите данных на таких устройствах весьма беспечно [11]. Некорректная организация антивирусной защиты редакционных информационных систем представляет серьезную опасность, так как инфицирование компьютеров вирусами чревато уничтожением или блокированием ценной информации или утечкой конфиденциальных данных.

Оптимизация результатов работы. Информационная безопасность не относится к факторам, определяющим образом влияющих на оптимизацию издания, его структуру, модель или систему публикаций. Однако можно говорить об опосредованном влиянии на эти характеристики, т.к. в итоге результаты работы СМИ оказываются зависимы от того, насколько эффективно решены управленческие задачи в сфере информационной безопасности. Как уже указывалось выше, следствием реализации информационных угроз могут быть не только финансовые потери, но и подрыв репутации издания как стабильно функционирующего и респектабельного. Можно говорить о том, что оптимизация результатов работы СМИ оказывается существенным образом зависима от того, насколько успешно осуществляется управление безопасностью редакционными информационными системами и ресурсами.

Таким образом, все основные задачи редакционного менеджмента должны решаться с учетом требований обеспечения информационной безопасности.

ЛИТЕРАТУРА

1. Гуревич С.М. Экономика отечественных СМИ : учеб. пособие / С.М. Гуревич. – М. : Аспект Пресс, 2004. – 288 с.

2. Ddos атака на популярное Российское интернет-издание. –(http://www.antiddos.biz/latest-news/ddos-ataka-na-populyarnoe-rossiyskoe-internet-izdanie).

3. DDOS атака на сайт информагентства URA.RU. –(http://www.uralnets.ru/news_item164.html).

4. DDoS-атака на сайт и закрытие газеты «Быстрый Нейтрон». – (http://z-city.ru/forum/viewtopic.php?f=1&t=4391).

5. Для атаки на сайт «Новой газеты» хакеры написали специальный вирус. Электронное представительство газеты «Жизнь гражданина России». – (http://www.gosgra.ru/articles/739/).

6. ИА «Хакасия» объявила о DDOS-атаке. Мнение специалиста. – Современная Хакассия. – (http://www.web19.ru/news/10/319/).

7. Милиционеры отказались возбудить дело по факту DDoS-атаки на сайт «Ведомостей». – Сайт газеты «Ведомости». –(http://www.vedomosti.ru/tech/news/959272/milicionery_otkazalis_vozbudit_delo_po_faktu_ddosataki_na_sajt_vedomostej)].

8. «МК» обратится в силовые структуры из-за хакерской атаки на свой сайт. – РИА «Новости». – (http://www.rian.ru/trend/hacker_mk_04122009/).

9. Полесков Константин. DDos-атака на сайт «Новой газеты». – (http://www.livejournal.ru/themes/id/27191).

10. Полесков Константин. DDoS-атака на сайт «Новой газеты» и Сетевой парламент. – Новая газета № 37 от 8 апреля 2011 г. – (http://www.novayagazeta.ru/data/2011/037/34.html).

11. Развитие информационных угроз в первом квартале 2011 года. – Сайт «Лаборатории Касперского». – (http://www.kaspersky.ru/news?id=207733480).

12. Реакция на выборы? Для атаки на сайт «Новой газеты» хакеры написали специальный вирус. Каспаров.Ru. Интернет-газета Гарри Каспарова. – (http://www.kasparov.ru/material.php?id=4D9DCD9CC9B77).

13. Сайт информационного агентства Trend был подвергнут хакерской атаке. – Сайт trend.az. – (http://ru.trend.az/news/society/1858792.html).

14. Сайт информационного агентства Trend подвергся хакерской атаке. – Сайт Day.az. – (http://news.day.az/hitech/261379.html).

15. Славина Ирина. Мощная хакерская атака на сайт газеты «Ведомости». Сайт «Неформат» / Ирина Славина. – (http://neformat.co.ua/index.php?nma=news&fla=stat&nums=2501).

16. Хакерские атаки на интернет-издание коммерсант.мд продолжаются. – (http://www.medialawca.org/node/8214).

17. Хакеры Кивалова продолжают DDOS-атаки оппозиционного интернет-издания «Спротив». – (http://motoshyna.livejournal.com/3230.html).

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.