КАДРОВАЯ БЕЗОПАСНОСТЬ ОРГАНИЗАЦИИ КАК ОБЪЕКТ УПРАВЛЕНИЯ

ДЖАБРАИЛОВ МАГОМЕД АХМЕДОВИЧ
ФГБОУ ВПО «Тамбовский государственный университет имени Г. Р. Державина»,
г. Тамбов, Российская Федерация, e-mail: magomedrambler@rambler.ru

В статье рассматривается кадровая безопасность в системе безопасности организации. Уточнены основные угрозы кадровой безопасности со стороны персонала организации и в его адрес, источники их возникновения и последствия реализации. Особое внимание уделено информационной безопасности организации. По итогам исследования был выявлен определенный дисбаланс в сфере защиты информации от утечек. С одной стороны, и руководители бизнеса, и рядовые сотрудники осознают важность информационной безопасности. С другой стороны, на практике информация оказывается чрезвычайно уязвимой. Тем не менее, позитивным является сам факт осознания проблемы и определенные шаги, направленные на ее решение. Изменения на рынке происходят все быстрее, и требование к скорости получения, обработки и анализа информации становится первоочередным, при этом бизнесмены проявляют готовность идти на дополнительные расходы ради своевременного получения необходимой информации. В условиях развивающегося бизнеса при сохранении жесткой конкуренции наступает необходимость нового способа получения информации о конкурентах. Такие возможности предоставляют сервисы для анализа их деятельности. В настоящее время взрывной рост численности аудиторий социальных медиа открыл большие возможности для развития бизнеса с использованием ресурсов социальных сетей. Сами социальные сети предлагают компаниям разнообразный функционал и инструментарий для достижения различных целей.

***Ключевые слова*: кадровая безопасность, информационная безопасность.**

С развитием в России рыночных отношений проблема безопасности бизнеса, то есть минимизации рисков и отражения угроз, выдвигается на первый план. Любая предпринимательская деятельность сопряжена с риском. Непредсказуемость ее деятельности и ее результатов может привести не только к нежелательному результату, но и к невосполнимому.

Безопасность предприятия зависит от различных обстоятельств. Ущерб может быть нанесен в результате стихийных бедствий, неблагоприятной экономической политики государства, непредсказуемых изменений конъюнктуры рынка, недобросовестных действий конкурентов, невыполнения контрагентами обязательств по оплате договоров, а также противоправными действиями сотрудников [1]. Работник может найти доступ практически ко всем активам предприятия, способен преодолеть систему охраны объекта, защиту баз данных, может просто услышать нужную информацию. Пока ученые непрерывно изобретают все лучшие и лучшие технологии защиты, делая все более трудным возможность использовать технические уязвимости, атакующие все чаще используют человеческий фактор [2].

Одной из составляющих системы безопасности является кадровая безопасность (иногда ее называют «кадровой и интеллектуальной»).

Кадровая безопасность – это комплекс мер, направленных на предотвращение и устранение угроз и рисков, а также негативных для экономического состояния компании последствий, связанных с работой и поведением персонала, его интеллектуальным потенциалом, трудовыми отношениями в целом [3].

Кадровая безопасность занимает главенствующее положение среди других элементов системы безопасности, так как персонал задействован во всех процессах, происходящих в компании.

Есть некоторое заблуждение, связанное с тем, будто бы кадровой безопасностью должна заниматься только служба безопасности. Поиск, отбор, прием, адаптация, увольнение персонала, ведение делопроизводства и т. д. – все эти вопросы, находящиеся в ведении службы персонала, в той или иной степени связаны с обеспечением безопасности. И каждое решение, принимаемое менеджером по персоналу либо усиливает, либо ослабляет безопасность компании по главной ее составляющей – кадровой [4].

По статистике, потери от несовершенства системы безопасности составляют от 6 до 9 % прибыли компании. Эти данные характеризуют лишь случаи умышленного нанесения ущерба собственными сотрудниками. Оценить масштабы потерь и упущенной выгоды в результате ошибок персонала, неграмотного использования ресурсов, непрофессионализма, бездействия, нелояльности и т. д. просто невозможно. И никакая служба безопасности не решит эти проблемы самостоятельно, без помощи подразделения, чья деятельность прямо направлена на работу с людьми. Эффективная организация работы служб по управлению персоналом в обеспечении кадровой безопасности может почти на 60 % снизить прямые и предотвратить косвенные убытки компании, связанные с человеческим фактором [2].

В последнее время все серьезнее заявляет о себе новая для страны проблемная зона – утечки информации на предприятии.

Компания Zecurion совместно с порталом Superjob провела исследование защищенности конфиденциальной информации в корпоративной среде, в котором были рассмотрены различные сценарии утечки информации.

Так же, как театр начинается с вешалки, информационная безопасность организации должна начинаться на самых ранних этапах найма сотрудников. Одной из простейших, но в то же время эффективных мер, является подписание соглашения о неразглашении конфиденциальной информации. Выяснилось, что более половины работников (53 %) подписывали такие соглашения при трудоустройстве, но это не мешает им передавать информацию по незащищенным каналам и выносить документы на уязвимых мобильных носителях. В ходе исследования было установлено, что чаще всего для этого используют флешки (49 %) и электронную почту (43 %).

Также во время исследования были выявлены категории наиболее ценной для компаний и самих сотрудников информации. Так, согласно последним отчетам ZecurionAnalytics, наибольшее количество внутренних инцидентов за последние 3 года связано с утечками персональных данных [клиентов, сотрудников] и финансовых сведений физлиц, в основном клиентов крупных банков. При этом, по мнению участников текущего исследования, наиболее ценной корпоративной информацией являются персональные данные (указали 28 % респондентов) и сведения о сделках и договорах с клиентами, партнерами и поставщиками (16 %) [5].

Еще одна проблема, которую вскрыло исследование – это пропасть между намерениями и реальной защищенностью информации. При том, что лишь 10 % топ-менеджеров и владельцев бизнеса сказали, что их компаниям не нужны специалисты по информационной безопасности, в реальности лишь немногие из них выделяют достаточно средств для создания отделов по защите от утечек информации.

По итогам исследования был выявлен определенный дисбаланс в сфере защиты информации от утечек. С одной стороны, и руководители бизнеса, и рядовые сотрудники осознают важность информационной безопасности. С другой стороны, на практике информация оказывается чрезвычайно уязвимой. Тем не менее, позитивным является сам факт осознания проблемы и определенные шаги, направленные на ее решение. Технические средства контроля информационных потоков становятся более удобными в обращении. Можно ожидать, что с развитием законодательства в области защиты информации и ростом осведомленности пользователей количество утечек корпоративной информации будет постепенно снижаться.

Для достижения превосходства в современной конкурентной борьбе важным моментом становится знание намерений конкурентов, изучение основных тенденций деловой и политической жизни, анализ предпринимательских рисков и других факторов, влияющих на предпринимательскую деятельность [6].

В настоящее время в условиях конкурентной борьбы в негосударственном секторе экономики существует два направления разведывательной деятельности:

– разведка, проводимая с легальных позиций, – «деловая разведка»;

– разведка, проводимая с нелегальных позиций, – «промышленный шпионаж».

Информационные технологии за последние 10-15 лет неузнаваемо изменили методы управления бизнес – процессами. Похоже у бизнесменов не вызывает сомнения тот факт, что достоверная и своевременно полученная информация имеет критически важное значение для выработки и осуществления рыночной стратегии и тактики [7].

Сеть Интернет позволила компаниям-производителям быстро устанавливать и развивать прямые контакты с потребителями продукции и услуг – как с населением, так и организациями-партнерами, а также оперативно реагировать на изменение спроса. Именно Интернет становится главным источником и каналом получения ценной информации о спросе и потребительских интересах, о поставщиках и конкурентах,

т. е. той деловой информации, которую невозможно получить традиционными методами.

Изменения на рынке происходят все быстрее, и требование к скорости получения, обработки и анализа информации становится первоочередным, при этом бизнесмены проявляют готовность идти на дополнительные расходы ради своевременного получения необходимой информации.

В условиях развивающегося бизнеса при сохранении жесткой конкуренции наступает необходимость нового способа получения информации о конкурентах. Такие возможности предоставляют сервисы для анализа их деятельности [2].

Рассмотрим некоторые сервисы подробнее.

SEMrush – сервис для анализа конкурентных сайтов, источников трафика, ключевых слов, по которым конкуренты продвигаются в Google. Аналогов у него много (например, российский SpyWords и американские Alexa и Compete), но SEMrush особенно хвалят за качество и точность данных. Если ввести на сайте поисковый запрос, можно получить информацию об аналогичных и схожих запросах и сразу определить слова-пустышки, уровень конкуренции, среднюю стоимость клика в AdWords, количество страниц по каждому запросу. Затем можно посмотреть, какие сайты лучше всего продвигаются по этому запросу, увидеть, как они это делают, сколько платят, какие ключевые слова приносят им больше всего трафика, и использовать это в собственных интересах. Сервис также покажет, насколько постоянен интерес к запросу, то есть он помогает понять, какие слова сейчас в тренде, а какие – нет.

С помощью SEMrush можно оценить трафик разных страниц, чтобы, например, сделать выводы о популярности конкретного продукта и понять, сколько на его продвижение уходит денег у конкурента. Он позволяет сравнивать до пяти сайтов одновременно по разным параметрам: количеству ключевых слов и рекламных объявлений, поисковому трафику, его оценочной стоимости и т. д. Сервис построит на основе этих данных график или круговую диаграмму, чтобы результаты были более наглядными. Недавно появилась функция «трекинга позиций», которая позволяет следить за ежедневными изменениями мест конкурентов в выдаче Google по важным для вас ключевым словам. Самый популярный тариф стоит 70 дол. в месяц.

TheWaybackMachine – уникальный проект, который хранит информацию о прошлом интернета. Благодаря WaybackMachine можно посмотреть, как выглядел сайт вашего конкурента месяц или даже пять лет назад и проанализировать изменения, которые он внес. Можно даже увидеть сайты, которые уже закрылись. Содержание страниц фиксируется не каждый день, но часто. Чтобы выбрать интересующий период времени, нужно просто вбить название домена в поисковую строку на сайте и отметить в появившемся календаре дату, когда делались «снимки».

Русский сервис с жутковатым названием «АдВсе.ру» и довольно хмурым интерфейсом помогает проанализировать рекламные кампании ваших конкурентов. Преимущество сервиса перед англоязычными аналогами в том, что кроме Google он работает и с «Яндексом». Сайт сначала предлагает определить, кто является вашим конкурентом, и показать, по каким запросам видна их реклама. Затем – на основе этих данных, сформировать отчеты.

Информация первого отчета может помочь уменьшить расходы на рекламу в поисковиках, которые, как известно, зависят от уровня конкуренции. Сервис позволяет оценить степень конкуренции: отчет дает адреса сайтов, чья реклама была найдена в результатах поиска «Яндекса» и Google в ответ на интересующие запросы.

Система IQBuzz фиксирует любое упоминание бренда вашего конкурента в соцмедиа. Даже если пользователь удалит информацию, она все равно останется в системе. Полученные сообщения можно разделить по тону: позитивные, негативные, смешанные и нейтральные. Сводный отчет показывает цельную картину для каждой группы: число сообщений в день, общий охват, число уникальных авторов и ресурсов, пик обсуждений, топ источников, блогов и авторов.

С помощью отчетов можно анализировать общую упоминаемость брендов за определенный период времени на различных площадках. IQBuzz помогает найти лидеров мнений, отследить пики интернет-активности, выстроить графики сравнения брендов по многим параметрам. Помимо всего прочего, можно выявить инфоповоды, которые сгруппируют документы по темам. Эта функция позволяет понять, что именно обсуждают люди.

Система SemanticForce ведет общий мониторинг инфополя и медийной активности конкурентов, причем не только в социальных медиа, но и в онлайн-СМИ. Можно настроить поиск по ключевым словам и фразам, мониторинг групп и страниц конкурентов в Facebook, «ВКонтакте», Google+, а также LinkedIn. Считается, что по «ВКонтакте» у системы одно из лучших покрытий на рынке. Она также сообщает о любых изменениях на страницах конкурентов, например, в ценовой политике, что помогает быть в курсе всех их новостей.

SemanticForce отслеживает активность сотрудников компании. С помощью технологии ProfileForce система по адресу электронной почты или одному из аккаунтов в соцсети находит другие аккаунты и страницы человека. Схожая технология есть у «Яндекса».

С помощью сервиса можно также отслеживать сайты с вакансиями, чтобы следить за кадровыми изменениями у компаний-конкурентов. Для полноценной конкурентной разведки необходимо мониторить не только организации, но и в целом свою отрасль, быть в курсе новостей и отслеживать появление новых игроков на рынке.

Примером использования системы является исследование, проведенное на основе данных, собранных при помощи системы SemanticForce.

Исследование основано на данных, собранных и проанализированных за полгода, относящихся к восприятию русскоязычными автовладельцами новой модели HyundaiSolaris.

Основой для исследования стали данные из форумов, которые мало кто видит из мониторинговых платформ и поисковых систем, однако часто именно на таких классических площадках для общения по интересам идут самые жаркие обсуждения того или иного продукта или бренда.

С помощью специальной технологии SemanticForce по мониторингу дискуссий были собраны также косвенные сообщения об объекте, в которых HyundaiSolaris не упоминается напрямую. Кроме того, был проведен анализ факторов и контекстов выбора.

В общем виде на основе подобного анализа можно сделать выводы по поводу осведомленности людей о продукте, о его наиболее сильных и слабых сторонах с точки зрения потребителей и главных конкурентах. Также возможно отследить пожелания клиентов и их предпочтения. Такого рода исследования по восприятию продуктовой линейки потенциально могут быть полезны бренд-менеджерам, менеджерам по маркетингу и PR, специалистам по работе с клиентами, так как позволяют взглянуть на продукт критическим взглядом непосредственного покупателя (потребителя).

SemanticForce постоянно проводит подобные исследования.

Одним из примеров является исследование восприятия смартфона HTC Incredible S русскоязычными потребителями в сети Интернет, проведенное в 2011 г.

В настоящее время взрывной рост численности аудиторий социальных медиа открыл большие возможности для развития бизнеса с использованием ресурсов социальных сетей. Сами социальные сети предлагают компаниям разнообразный функционал и инструментарий для достижения различных целей.

Центры управления социальными медиа (SocialMediaCommandCenter, SMCC) уже давно успешно используются десятками компаний-лидеров западного рынка и привлекают внимание большого количества пользователей. По нашим прогнозам в 2013 г. аналогичные решения появятся и на рынке стран СНГ.

Аманда Нельсон (AmandaNelson), контент-менеджер и главный редактор блога SalesForce MarketingCloud, посвященного центрам управления социальными медиа, описывает 15 примеров использования подобных центров известными зарубежными брендами и организациями [5]. Необходимо использовать центры управления социальными медиа, чтобы:

– поддерживать связь с ключевыми лицами, принимающими решения;
– дать руководителю взглянуть на «состояние здоровья» бренда онлайн;
– оставаться на связи;
– использовать как платформу для антикризисных действий;
– обеспечивать контент-стратегию и развитие компании;
– выявлять ситуации при их возникновении для оперативного реагирования;
– изменить способ ведения бизнеса с клиентами к лучшему;
– следить за внешней средой;
– изменять общественное восприятие и характер общения;
– быть полезным ресурсом;
– увеличивать количество положительных упоминаний о вашем бренде;
– транслировать информацию для клиентов;
– быть голосом следующего отраслевого события;
– делиться метриками быстрее и в режиме реального времени;
– управлять социальными медиа из любой точки мира.

Таким образом, анализ сайтов в интернете – это ежедневная работа, с которой приходится сталкиваться аналитикам, CEO оптимизаторам и менеджерам интернет-проектов. Особенный смысл она приобретает, когда речь идет об анализе сайтов-конкурентов. Все представленные сервисы, помогут упростить эту задачу.

Так же, благодаря применению новых технологий служба, «деловой разведки» фирмы получает возможности:

– доступа в реальном времени ко всем информационным массивам, описывающим направления деятельности собственной фирмы и фирм-конкурентов;

– оперативного получения информации по конкретным вопросам;

– доступа к информации, хранящейся в удаленных архивах.

Литература

1. Радюкова Я. Ю., Шамаев И. Н. Экономическая безопасность страны как многоуровневая система элементов и отношений // Социально-экономические явления и процессы. Тамбов, 2011. № 1-2. С. 194-198.
2. Данченок Л. А. Маркетинг в социальных медиа. Интернет-маркетинговые коммуникации. СПб., 2013.
3. Алавердов А. Р. Управление кадровой безопасностью организации. М., 2010.
4. Соломанидина Т. О., Соломанидин В. Г. Кадровая безопасность компании. М., 2011.
5. Открытые Системы: сетевой журнал. 2013. URL: http://www.semanticforce.net/ru
6. Водянова В. В. Экономическая безопасность. Системное представление. М., 2010.
7. Радюкова Я. Ю., Кожевникова Т. М., Астахов К. В. Эпистемология угроз экономической безопасности России в условиях глобализации // Science and Education: materials of the IV international research and practice conference, Vol. I, Munich, October 30rd-31st, 2013/ publishing office Vela Verlag Waldkraiburg. Munich, Germany, 2013. С. 223-230.

References

1. Radyukova Ya. Yu., Shamaev I. N. Ekonomicheskaya bezopasnost' strany kak mnogourovnevaya sistema elementov i otnoshenij // Sotsial'no-ekonomicheskiye yavleniya i protsessy. Tambov, 2011. № 1-2. S. 194-198.
2. Danchenok L. A. Marketing v sotsial'nykh media. Internet-marketingovye kommunikatsii. SPb., 2013.
3. Alaverdov A. R. Upravleniye kadrovoj bezopasnost'yu organizatsii. M., 2010.
4. Solomanidina T. O., Solomanidin V. G. Kadrovaya bezopasnost' kompanii. M., 2011.
5. Otkrytye Sistemy: setevoj zhurnal. 2013. URL: http://www.semanticforce.net/ru
6. Vodyanova V. V. Ekonomicheskaya bezopasnost'. Sistemnoye predstavleniye. M., 2010.
7. Radyukova Ya. Yu., Kozhevnikova T. M., Astakhov K. V. Epistemologiya ugroz ekonomicheskoj bezopasnosti Rossii v usloviyakh globalizatsii // Science and Education: materials of the IV international research and practice conference, Vol. I, Munich, October 30rd-31st, 2013/ publishing office Vela Verlag Waldkraiburg. Munich, Germany, 2013. S. 223-230.

* * *

PERSONNEL SECURITY OF THE ORGANIZATION AS OBJECT OF MANAGEMENT

DZHABRAILOV MAGOMED AKHMEDOVICH
Tambov State University named after G. R. Derzhavin,
Tambov, the Russian Federation, e-mail: magomedrambler@rambler.ru

In article the author considered personnel security in a security system of the organization. He specified the main threats of personnel security from the staff of the organization and in its address, sources of their emergence and a consequence of realization. The author paid the special attention to information security of the organization. Following the results of research the author revealed a certain imbalance in the sphere of information security from leaks. On the one hand, both heads of business and ordinary employees realize importance of information security. On the other hand, in practice information is extremely vulnerable. Nevertheless, the fact of understanding of a problem and certain steps directed on its decision is positive. Changes in the market happen all quicker, and the requirement to the speed of receiving, processing and the analysis of information becomes prime, thus businessmen show readiness to go to the additional expense for the sake of timely obtaining necessary information. In the conditions of the developing business at preservation of fierce competition there comes need of a new way of obtaining information on competitors. Services for the analysis of their activity give such opportunities. Now the explosive growth of number of audiences of social media opened great opportunities for development of business with use of resources of social networks. Social networks offer the companies various functionality and tools for achievement of various purposes.

Key words: personnel safety, information security.