В. Герасимов, Исполнительный директор Информационной группы "Интерфакс"

Защита репутации бизнеса: стратегия и тактика

(журнал "Директор по безопасности", январь 2016)

РЕПУТАЦИОННЫЙ РИСК, учитывая масштабы его потенциального негативного влияния на бизнес, входит в число стратегических. Источники угроз «доброму имени» столь многообразны, что думать об их минимизации обязаны сегодня и топ- менеджеры, и пресс-секретари, и не в последнюю очередь сотрудники служб безопасности. Несмотря на непредсказуемость и многочисленность репутационных угроз, они вполне поддаются классификации, измерению и мониторингу, ВЫРАБОТАНЫ ПРОВЕРЕННЫЕ НА ПРАКТИКЕ СПОСОБЫ ЗАЩИТЫ ОТ НИХ.

Технология превращения мухи в слона

Газетой можно убить муху, а можно и человека – говорили в XIX веке. Или компанию – добавили бы сегодня, вспомнив десяток последних случаев, когда крупнейшие мировые корпорации оказывались на грани выживания из-за ущерба деловой репутации.

Репутация – это неосязаемый актив, отражающий восприятие компании окружающей экономической, политической и социальной средой, стимулирующий клиентов продолжать пользоваться услугами этой компании.

Репутационные вызовы – это «риск рисков». Являются эти вызовы, как правило, следствием каких-то конкретных проблем, связанных с нарушением норм безопасности, этики или регулирования, требований к качеству товаров или услуг. Однако последствия этих проблем разрастаются до огромных и часто непропорциональных масштабов, будучи усилены социальными сетями, общественным мнением и СМИ.

Самые яркие примеры того, как это происходит, приходят к нам с Запада. И это понятно. Репутационные кри- зисы обходятся компании тем дороже, чем выше стоимость ее бренда и чем важнее бренд для ведения ее бизнеса.

На Западе, по прикидкам экс- пертов, 70–80 % рыночной стоимости приходится именно на бренд, интеллектуальный капитал, гудвил. Средства массовой информации, общественные организации многочисленны и значительно более независимы, чем в России. Поэтому в развитых странах деловая репутация корпораций оказывается особенно уязвимой.

В России оценки компаний невысоки, роль нематериальных активов сильно ниже, а доверие в бизнесе в целом – в дефиците. Тем не менее репутационные риски все чаще реализуются и в России, хотя и с учетом национальной специфики.

Национальные особенности

Банк России рекомендует банкам вырабатывать принципы управления риском потери деловой репутации, «изучать влияние факторов риска потери деловой репутации на деятельность и финансовое состояние» организации.

Антиотмывочный закон (115-ФЗ) обязывает широкий круг финансовых структур «принимать обоснованные и доступные в сложившихся обстоятельствах меры по определению целей финансово-хозяйственной деятельности, финансового положения и деловой репутации клиентов».

Наконец, репутационные риски волнуют директора практически любой структуры, деятельность, товары, услуги которой обсуждают (или могут вдруг начать обсуждать) в сети или в медиа.

Россия, таким образом, тут в общемировой струе. Однако перечень главных рисков у нас несколько иной. Реакция бизнеса и потребителей на них также отличается.

Дефектные подушки безопасности, произведенные японской фирмой Takata, стали причиной отзывов 25 млн автомобилей самых разных марок и череды громких скандалов. Японской Toyota пришлось заплатить 1,1 млрд долл. в качестве штрафа за череду масштабных отзывов автомобилей, которые подорвали репутацию компании по всему миру. В случае с Volkswagen «дизельгейт» привел к тому, что компания впервые за 15 лет показала убыток, ей пришлось извиняться и каяться, расстаться с десятками менеджеров, включая CEO…

Отзывал машины и российский АвтоВАЗ – из-за проблем с двигателями, дефектов топливной системы, неполадок в электронике. Однако ни громких разоблачений в прессе, ни шумных раскаяний от самого завода, ни отставок не случилось. То ли не ожидают ничего такого у нас от АвтоВАЗа, то ли потребители всем довольны, то ли все оказались рады уже самому желанию автозавода исправлять недостатки.

Другое дело – торговля. Тут российские потребители в целом не менее требовательны, чем западные.

Доставалось в последнее время сети «Магнит». То Роспотребнадзор штрафует ее на 30 тыс. рублей за незаконную продажу санкционного сыра, то в Барнауле против сотрудников магазина возбуждают уголовное дело за незаконное удержание в подсобке школьниц, заподозренных в краже шоколада. Апофеозом стала история со смертью пенсионерки-блокадницы, которую сотрудники «Магнита» в Санкт-Петербурге обвинили в краже трех пачек масла, сдали в полицию, где она и умерла от сердечного приступа. Как установила проверка прокуратуры, кражи не было.

Сам «Магнит» выступил с извинениями только через 3 дня, уже факти- чески не добровольно, после того, как извинений потребовали влиятельные общественные организации. Глава компании Сергей Галицкий сначала настаивал, что его подчиненные действовали строго по инструкции, и лишь потом признал, что лучше бы они поступили по-другому.

Эта история вызвала широкий общественный резонанс (который, впрочем, довольно быстро сошел на нет). Директора магазина сначала осудили, но потом амнистировали. При этом магазин работает до сих пор, покупатели активно ходят в него, несмотря на подмоченную репутацию.

Если говорить о реакции СМИ, то о жестокосердных сотрудниках «Магнита» и его службы безопасности не отписался только ленивый. В блогах и сообществах были инициированы бойкот магазина и показательная доставка к его дверям пачек масла, ставших причиной смерти пенсионерки. Но скоро тема иссякла, интерес «четвертой власти» к теме оказался сиюминутным.

Еще больше сходств можно найти между действиями российских и зарубежных компаний, если говорить о сфере IT.

Компании Apple, которая в целом имеет уникально хорошую репутацию, пришлось извиняться за глупейшие ошибки в навигационных картах. Полиция сообщала о случаях, когда приходилось спасать людей, заблудившихся из-за неправильных данных, блогеры глумились над тем, где оказались на картах Apple известные всем места. Главе Apple Тиму Куку пришлось признать, что компания напортачила, пообещать все исправить. Сделано это было практически молниеносно.

8 октября 2015 года «Яндекс» перезапустил сервис «Кинопоиск», но, как оказалось, сделал это неудачно. Пользователям не понравились изменения на сайте и его нестабильная работа. Шквал критики привел к тому, что уже 12 октября компания вернула старую версию сайта. Была уволена часть команды «Кинопоиска».

Для банка (и российского, и зарубежного) плохая репутация почти всегда равняется потере какого-то числа клиентов, поэтому руководство и акционеры банка стараются ситуацию не пускать на самотек. Пожалуй, в этой сфере мы почти совсем не отличаемся от зарубежных реалий.

…Банк «Тинькофф кредитные системы» попытался взыскать через суд проценты за пользование кредитом с предпринимателя из Воронежа Дмитрия Агаркова. По ходу дела выяснилось, что бизнесмен исправил кредитный договор, вписав в него мелким шрифтом дополнительные условия. Процент за пользование кредитными деньгами он установил в 0 %, а за каждое изменение условий обязал ТКС-Банк выплачивать миллионные штрафы. Банк, не ожидая подвоха, измененный договор не глядя подписал. Клиент решил взыскать с банка 24 млн руб. штрафов, банк стал грозить непокорному клиенту тюрьмой...

Но вдруг все изменилось: стороны по- мирились, свои претензии отозвали, банк даже выпустил для Агаркова специальную дебетовую карту. Эксперты прочили бизнесмену легкую победу в суде, ведь договор был полностью законен. Таким образом, жест доброй воли со стороны банка помог ему спасти репутацию, если уж не деньги.

Однако общая тенденция пока такова, что российские компании в целом реагируют на репутационные кризисы заторможенно и оказываются к ним не готовы. Сначала, судя по последним примерам, у руководства возникает предположение, что, может быть, «и так рассосется», что «это все журналисты нагнетают» и что можно «договориться, чтобы это прекратилось». И лишь потом (если не рассосалось и не прекратилось) компании приходит- ся давать публичные объяснения или уточнять предыдущие заявления.

При этом бывает, что компании опровергают наличие проблем до последнего, даже если для этого им приходится лгать, что называется, в глаза.

Фронт без флангов

Репутационные риски многообразны, однако на основании примеров последних лет все же можно перечислить основные:

- операционные риски (аварии, качество продукции и услуг);
- коррупция, нарушения в сфере законодательства о госзакупках;

- мошенничество, невыполнение обязательств, нарушение бизнес-этики;
- финансовые проблемы, банкротство;
- хакерские атаки, утечка информации о клиентах;
- судебные разбирательства;
- нарушение законодательства или норм этики сотрудниками;
- трудовые споры;
- обвинения в инсайдерской торговле, манипулировании, отмывании денег;
- нарушение экологического законодательства;
- уклонение от уплаты налогов.

Какие из этих рисков чаще всего реализуются на Западе? По опросам Deloitte, это вопросы этики и культуры (integrity) организации, включая случаи мошенничества, коррупции, подкупа (55 %). На втором месте – киберриски и другие риски безопасности (45 %), третьем – риски, связанные с продуктами, услугами (43 %).

В России все несколько по-другому. Если проанализировать события последних лет, то на первом месте по частоте оказываются риски, связанные с мошенничеством, хищениями, нецелевым использованием бюджетных средств (35 %). На втором (около 25 %) – проблемы с качеством товаров и услуг. Далее идут риски нарушения законодательства (10 %), примерно по 5 % приходится на нарушение норм этики, финансовые риски, аварии.

Киберриски репутацию наших компаний пока затрагивали мало. Максимум компании признают, что их сервисы были недоступны из-за DDos атаки или мошенники украли деньги с нескольких кредитных карт. Однако ни разу мы не слышали публичных признаний, сколько данных потребителей было в итоге украдено. Добровольное раскрытие информации у нас в таких случаях пока не практикуется.

Зато риски, связанные с коррупцией, у нас реализуются заметно чаще, чем на Западе. При этом инициатором разоблачений тут является, как правило, само государство (иногда в лице самого президента, как было в случае с энергетическими компаниями в 2011 г.), обвинения в этих случаях подхватывают все без исключения СМИ.

Поскольку государство в России всесильно, то извинения, контраргументы и оправдания в этих случаях оказываются, как правило, уже бессмысленными.

На Западе последствия репутационных кризисов – снижение выручки, потеря стоимости бренда, регулятивные меры (штрафы), падение цены акций. По данным опросов Deloitte, в 41 % случаев кризис ведет к потере выручки. Столько же респондентов назвали главным последствием снижение стоимости бренда, 37 % указали последствия на разного рода действия регулирующих органов в отношении компании.

У нас за кризисами чаще всего следуют карательные действия правоохранительных или надзорных органов, нередко – смена собственника (как было в случае с «Уралкалием» после аварии и ареста ее руководителя). Российские же потребители, в отличие от западных, чаще всего оказываются более снисходительными к опростоволосившимся компаниям.

Есть в России много структур, которые больше зависят не от рынка, а от государства. Но даже и для них «доброе имя» все в большей степени имеет ценность.

Эти опасные соцсети

Распространение социальных медиа привело к тому, что бизнес, транслируя свои оценки, вынужден теперь напрямую конкурировать с коллективным мнением потребителей в соцсетях.

Социальные сети могут молниеносно ввергать компании в репутационные кризисы – причем еще до того, как сами менеджеры компаний узнают о возникшей проблеме. В этой части ситуация в России мало чем отличается от общемировой.

Телеведущая Ксения Собчак в 2008 г. опубликовала историю о том, как пассажирам рейса Москва–Нью-Йорк удалось «ссадить» с борта пьяного пилота. Пост произвел настоящий фурор, его перепечатали СМИ, в том числе иностранные, обсуждали на радио и ТВ. Авиакомпании пришлось оправдываться: пилот был не пьян, а болен. Но негативное для компании общественное мнение по этому вопросу уже сложилось.

Сбербанку припоминают, как в соцсетях кто-то из его сотрудников пошутил: «Народный лайфхак: Если на стене мелом написать «Сбербанк», у стены образуется очередь из 30 пенсионерок». Шутка вызвала воз- мущение в сети, банку пришлось извиняться и объяснять, что это был «народный юмор» и что он совсем не против пенсионеров.

Для банка (и российского, и зарубежного) плохая репутация почти всегда равняется потере какого-то числа клиентов, поэтому руководство и акционеры банка стараются ситуацию не пускать на самотек. Пожалуй, в этой сфере мы почти совсем не отличаемся от зарубежных реалий

Несть числа таким примерам и на Западе. Вот недовольный собственник машины Maserati нанял группу молодых людей, чтобы они разнесли в пух и прах новенькое спортивное авто. Соответствующее видео приобрело в сети широкую популярность, и Maserati пришлось долго и упорно оправдываться.

Это наглядно показывает, как важно для компаний оперативно отслеживать соцсети и следить за поведением в них сотрудников. Скорость реакции на негатив может сократить или, напротив, умножить репутационный ущерб. Наличие правил поведения в соцсетях помогает предотвратить утечку негативной информации и повысить ответственность сотрудников за свои действия.

Глобальные компании идут по пути создания ситуационных центров, с помощью которых ведется постоянный мониторинг важных сообщений в социальных сетях. Например, в MasterCard соцсети постоянно отслеживают четыре сотрудника. Перед запуском новых продуктов проводится целенаправленный мониторинг десятков тысяч постов и комментариев.

Некоторые «передовики» утверждают, что научились противостоять волнам негатива и даже использовать их в собственных интересах. Так, производитель электромобилей Tesla Motors столкнулся с серией сообщений о возгораниях электромобилей. Однако с помощью тех же соцсетей компании, по ее утверждению, удалось стабилизировать ситуацию и снять опасения потребителей. «Без социальных сетей нам бы не удалось исправить это искаженное восприятие», – сказал на конференции для инвесторов глава компании.

Многие крупные российские компании также поставили соцсети на службу собственному имиджу и ведут постоянный и детальный мониторинг «ВКонтакте», Facebook, Twitter. В своих аккаунтах они общаются с пользователями, выкладывают новости, оперативно отвечают на претензии и «горячие вопросы» следуя при этом жестким правилам.

Понятие деловой репутации в российской деловой практике

Деловая репутация может оцениваться как качественными, так и количественными показателями. В качестве примера количественного показателя можно назвать стоимостную оценку деловой репутации, используемую в российской экономической практике при бухгалтерском учёте нематериальных активов: стоимость деловой репутации определяется как разница между текущей рыночной ценой, предлагаемой продавцу (владельцу) актива при приобретении предприятия как имущественного комплекса (в целом или его части), и стоимостью всех активов и обязательств по бухгалтерскому балансу на дату его покупки (приобретения), т. н. Гудвилл (понятие используемое в зарубежной деловой практике).

Преимущества активной обороны

В эпоху массовых социальных коммуникаций и глобализации репутационный риск может возникнуть ниоткуда, как черт из табакерки, и развиваться молниеносно.

Поэтому, во-первых, важна скорость получения информации и реакции на нее, иначе информационную повестку будут определять другие. Во-вторых, важно помнить о сигналах, которые в случае кризиса необходимо коммуницировать вовне:

- озабоченность: «видимо, что-то пошло не так, мы сожалеем и озабочены»;
- все под контролем: «руководство все держит под контролем, взаимодействует с властями»;
- решимость: «мы исправим ситуацию, предпримем необходимые шаги, это не повторится».

Показательна недавняя история с инвалидом-колясочником, которую сотрудники «Аэрофлота» не пустили на рейс. Модель Светлана Нигматуллина, которая возвращалась в Калининград с московской Недели высокой моды, провела шесть часов в московском аэропорту из-за того, что ее коляска была признана слишком тяжелой. В результате домой она все-таки улетела, но на другом рейсе, и потом решала вопрос с поездкой из Калининграда до родного города, так как встречавшие ее уже уехали из аэропорта.

После того как эта история была обнародована, руководство «Аэрофлота» связалось с ней, принесло личные извинения и пригласило на заседание общественного совета, чтобы обсудить, как улучшить сервис для маломобильных пассажиров.

В некоторых случаях компаниям удается даже полностью взять на себя инициативу. Например, эксперты позитивно оценили действия Siemens AG в коррупционном строительном скандале в Бразилии. Компания сама обнаружила признаки нарушений, сообщила об этом властям и активно сотрудничала со следствием.

В каждом кризисе обычно есть возможность для успешного выхода из него, если его искать.

Еще один важный элемент защиты – обратная связь, позволяющая оперативно оценивать эффективность предпринимаемых в кризисной ситуации информационных шагов, КПД пресс-релизов и заявлений компаний.

Иногда первое ощущение, что кризис миновал и можно вздохнуть с облегчением, оказывается обманчивым. То, как компания на практике реагирует на критику, компенсирует убытки или отвечает на жалобы клиентов, может быть поводом для второй волны негатива, проблема может неожиданно вновь разрастись. Поэтому не стоит торопиться закрывать тему и прекращать мониторинг ситуации.

Полезны бывают и отвлекающие маневры. Например, хорошие информационные поводы: получение наград, спонсорские контракты, интервью руководства.

Однако следует всегда помнить, что ситуация может развиваться и по наихудшему сценарию.

Потенциальный масштаб вызовов можно проанализировать на примере киностудии Sony Pictures (владеет брендами Columbia Pictures, MetroGoldwyn-Mayer), которая подверглась в 2014 г. хакерской атаке. Самое первое публичное сообщение Sony Pictures об атаке было успокаивающим: «Мы ведем расследование одной IT-проблемы».

Проблема, однако, оказалась серьезной. Хакеры раскидали по Сети ворохи украденной информации. Стала достоянием гласности внутренняя переписка руководителей студии, финансовая отчетность, коммерческие секреты, график выхода лент – в общей сложности до 100 терабайт информации.

Среди появившихся в свободном доступе данных были телефонные номера более чем 47 тыс. человек, информация о зарплате о более чем 15 тыс. нынешних и бывших сотрудников компании. Оказались украдены 5 фильмов, включая один еще не вышедший в прокат.

Многие СМИ воспользовались утечкой данных Sony Pictures и опубликовали фрагменты внутренней переписки, в том числе те, где обсуждались такие кинозвезды, как Анджелина Джоли, Леонардо Ди Каприо и другие.

Сопредседатель совета директоров компании Эми Паскаль и продюсер Скотт Рудин вынуждены были принести извинения президенту США Обаме за шутки, допущенные ими в личной переписке. В своих письмах они, в частности, шутили о том, какие фильмы могли бы понравиться президенту и приводили в пример картины, главные роли в которых играли чернокожие актеры. С. Рудин извинился перед актрисой Анджелиной Джоли за то, что назвал ее «испорченным ребенком».

Оказалась нарушена работа 75 % серверов компании, были стерты важные данные, на полное восстановление работоспособности систем потребовалось несколько недель. Пришлось разбираться с сотрудниками, данные которых были скомпрометированы.

Sony Pictures, чтобы положить конец использованию в сети информации, полученной в результате кибератак, наняла адвоката и написала грозные предупреждения крупнейшим СМИ. Но эти шаги оказались запоздалыми и только вызвали еще одну волну язвительных комментариев со стороны журналистов.

Из-за угроз хакеров Sony Pictures решила отменить массовый показ фильма «Интервью» (The Interview), в котором рассказывается о попытке покушения на северокорейского лидера. За это решение она подверглась публичной критике со стороны самого президента США, звезд Голливуда и многих политиков. Ведь получилось, что компания пошла на поводу у тер- рористов. Руководству Sony Pictures пришлось отвечать на критику Обамы и оправдываться.

Как выяснилось, ряд своих действий Sony Pictures в спешке толком просто не объяснила. Так, сообщение об отмене показа ленты в крупных сетях все восприняли как полную капитуляцию компании (хотя Sony Pictures, как потом выяснилось, уже вела активные переговоры о прокате «Интервью» через интернет-кинотеатры).

На Западе эксперты говорят, что компании не должны бояться раскрывать информацию о хакерских атаках. Напротив, нужно ясно и оперативно заявлять о своей позиции в отношении интернет-преступников и защиты данных сотрудников, просить помощи у государства и т. д.

Компании активно озабочены укреплением электронной защиты. Это правильно, но эксперты по безопасности, указывая на уроки истории с Sony, рекомендуют менеджерам вообще не пользоваться электронной почтой для обсуждения конфликтных или личных тем, говорить обо всем этом с глазу на глаз.

Уязвимость крупных бизнес-структур иногда связана также с чрезмерной сложностью и устареванием внутренних электронных систем. Здесь рецептом может быть разумное упрощение этих систем и их модернизация.

Еще один вывод: в компаниях должна действовать система уничтожения ненужной информации. «Лишние» электронные письма, чаты – все это дополнительный риск, показывает история с Sony.

Хорошая репутация – лучшая защита

Помогает защититься от рисков хорошая репутация. По всем опросам, потребители, акционеры не очень верят позитивной информации про компании, которым они не доверяют, и наоборот.

Доверие к британской компании BP было поколеблено еще до масштабной аварии в Мексиканском заливе, и катастрофа подтвердила опасения, что компания не уделяет должного внимания вопросам безопасности. С другой стороны, в случае с Apple доверие к бренду позволяет относительно легко минимизировать возникающие угрозы.

Именно поэтому эксперты настоятельно рекомендуют регулярно оценивать текущий уровень репутации компании, в том числе со стороны. И делать из этого выводы.

К репутационным кризисам надо также готовиться. Во-первых, выявлять возможные угрозы и уязвимости, в том числе в контексте отрасли и с учетом опыта конкурентов. Учитывать репутационные факторы при принятии тех или иных важных управленческих решений, в том числе в сфере безопасности.

Например, в США одной из тенденций является ужесточение регулирования глобальных банков, и ряд крупных кредитных организаций стали больше уделять внимания превентивным шагам. Действуя на опережение, J.P. Morgan & Chase Co. выпустила 90-страничный документ «Как мы делаем бизнес».

Компании нужно иметь под рукой подготовленных специалистов, которые смогут выехать на место, принимать быстрые решения, наладить коммуникации и внушать доверие.

Самое важное – оперативный и постоянный мониторинг информационного пространства и других угроз. Чем скорее конкретный риск будет выявлен, тем больше шансов на успешное разрешение кризиса.

Чтобы готовить менеджеров к новым угрозам, PwC выпустила недавно специальную деловую игру Game of Threats, которая позволяет осознать быстроту и сложность событий в случае взлома информационной системы компании. Цель – научить руководителей действовать быстро и адекватно, предотвращая развитие ситуации по наихудшему сценарию. Участники игры могут меняться ролями, чтобы лучше понимать психологию и мотивацию хакеров.

Бизнес увеличивает инвестиции в механизмы управления репутационными рисками, свидетельствует опрос Forbes Insights для Deloitte.

Более половины (57 %) из опрошенных 300 глобальных компаний вкладываются с этой целью в развитие технологий (аналитика, инструменты мониторинга прессы и бренда). Они также работают над улучшением своих возможностей сфере кризис-менеджмента и планирования сценариев. Правда, треть (36 %) компаний сказали, что пока не занимаются разработкой сценариев из серии «что если…».

Тут придется признать, что есть риски, к которым практически невозможно подготовиться. Например, к событиям, которые находятся все зоны контроля конкретной компании: к возникновению проблем у поставщиков (как в случае с европейскими модными домами, которые оказались вынуждены оправдываться из-за обрушения фабрики одежды в Бангладеш), или к природным катастрофам, атакам конкурентов. Есть примеры непредсказуемых действий работников (как в случае с пилотом разбившегося самолета Germanwings или нерадивым трейдером Societe Generale).

Знай своего клиента

Важным и в финансовой (где действуют специальные требования в сфере ПОД/ФТ), и в нефинансовой сфере является постоянная проверка контрагентов. Не является ли компания однодневкой (что может быть чревато налоговыми проблемами)? Кем являются конечные бенефициары (не воз- никает ли коррупционных рисков)? Нет ли аффилированности с компаниями и гражданами, находящимися в зоне риска (нет ли угрозы, что компания-партнер может быть вовлечена в операции по отмыванию денег)?

Для ответов на эти вопросы компании и банки используют такие системы, как СПАРК, X-Compliance, данные D&B (если речь идет о зарубежных партнерах). В каждой из этих систем есть инструментарий, включая рейтинги и скоринги, сервисы для скрининга и мониторинга, которые позволяют давать конкретные ответы на поставленные вопросы.

Проверка контрагентов – это как раз сфера ответственности служб безопасности. Однако, как показывает практика общения со специалистами в этой сфере, они часто игнорируют мониторинг неструктурированных источников информации, в первую очередь медиа.

Системы медиамониторинга, такие как СКАН, позволяют автоматизировать отслеживание негатива сразу по всему кругу источников и всему интересующему списку компаний. Причем в число этих источников входят и тысячи СМИ, и десятки тысяч сайтов, и база данных решений арбитражных судов и т. д. Чтобы не утонуть в море публикаций, специалист по безопасности бизнеса может настроить фильтр, допустим, только по темам («мошенничество», «коррупция») или только на негатив.

Недавно в нашей практике был случай, когда компания узнала об обыске в офисе своего крупного партнера из мониторинга новостей в тот самый день, когда намечалось подписание с этим партнером крупного контракта.

В России все больше компаний приходят к осознанию, что успешность их бизнеса в огромной степени зависит от лояльных потребителей, надежных партнеров, хорошего бренда, позитивного (или хотя бы никакого) информационного фона. Все эти компоненты требуют постоянного, практически ежедневного контроля: репутация создается годами, а потерять ее можно за один день.